Department of Home Affairs
Australian Government
Discussion paper submission - Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

27 August 2025

Brandsec Horizon 2 Cyber Security Policy Discussion Paper Submission

Dear Sir/Madam,

I welcome the Charting New Horizons - Horizon 2 Cyber Security Policy and, in particular, the continued focus on Shield 5: Sovereign Capabilities. The commitment to foster robust local solutions and strengthen Australia's cyber workforce is exactly what is needed if we are to reduce dependence on foreign providers and build a resilient national cyber sector.

Despite this clear policy direction, there remains a persistent gap between strategy and practice. While Horizon 2 highlights the importance of sovereign capability, procurement outcomes continue to favour long-standing overseas incumbents. This has the unintended effect of constraining the growth of capable Australian firms and slowing the development of a sustainable domestic skills pipeline.

By way of context, Brandsec Pty Ltd is an Australian-owned cyber security business specialising in online brand and phishing protection. We are trusted by some of the nation's most recognisable enterprises, including banks, airlines, and digital service providers, to safeguard their customers from phishing, impersonation, and online fraud. Our enforcement platform, Unphish, was developed with the support of the Australian Government and is a practical example of sovereign innovation being applied at scale.

Recent procurement outcomes illustrate the structural issue. High-value cyber security service contracts continue to be awarded offshore - even where sovereign solutions exist and are already proven in the market. To be clear, agencies are acting appropriately within the current rules and achieving their immediate objectives. The problem lies with the framework itself, which does not require sovereign capability to be identified, prioritised, or weighted in decision-making. One recent procurement illustrates the point. A phishing website takedown service contract (CN ID: CN3984183-A1) was awarded to a long-standing overseas incumbent at a cost exceeding $9 million. To be clear, the agency acted entirely within the current rules and achieved its objectives. The issue is not with the decision itself but with the framework: there was no requirement to prioritise sovereign capability, even though Australian solutions were operating at scale. This outcome highlights how policy intent can be undermined in practice, not through malice or error, but through the absence of structural mechanisms to prioritise and support sovereign providers and technology. The consequences of this misalignment are tangible:

In the short term - sovereign providers are excluded from critical opportunities; Australian analysts and engineers lose the chance to build frontline skills; and confidence in government's stated commitment to sovereign capability is weakened.

In the long term - industry confidence erodes. R&D investment declines, and the nation risks losing the very talent that has deliberately chosen to remain in Australia to defend its consumers and institutions. Instead of building resilience, we risk entrenching dependency on offshore providers whose decision-making and R&D occur outside our jurisdiction.

This issue is not unique to cyber security. A recent ANAO audit found that Defence was not consistently upholding its own requirements to maximise Australian industry participation. Without reform, sovereign capability risks remaining an aspiration on paper rather than an operational reality. Horizon 2 provides the opportunity to change that, ensuring that policy intent is matched by procurement practice, and that Australia invests in the growth of its own sovereign depth rather than the capacity of others.

This submission focuses on Shield 5: Sovereign Capabilities, addressing the gap between policy intent and procurement practice, and provides recommendations on how government can strengthen Australia's cyber workforce (Q39) and prioritise sovereign capabilities for growth (Q44).

Department of Home Affairs
Australian Government
Discussion paper submission - Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Summary of Key Recommendations

1) Accountability in procurement - building trust and transparency
Agencies should be required to publish clear justifications when sovereign providers are bypassed. This would build public and industry confidence that procurement decisions are consistent with Horizon 2's commitment to sovereign capability.

2) Dual-track procurement model - developing capacity while managing risk
Where an international incumbent is engaged, a parallel contract should be awarded to a sovereign Australian firm. This approach reduces risk for government by ensuring continuity of service, strengthens competition, and provides local providers with real-world delivery experience, aligning with Horizon 2's goal of deepening sovereign capability.

3) Short-term foreign contracts - keeping competition open
Where foreign providers are selected, contract terms should be capped at a maximum of 24 months. This avoids long-term lock-in and ensures sovereign firms have regular opportunities to compete, driving continuous innovation and growth.

4) Sovereign-by-default for critical defensive functions
For frontline services such as phishing detection, takedown, and DNS abuse enforcement, procurement should default to sovereign capability unless a compelling, published case is made otherwise. This directly supports Horizon 2's focus on resilience and preparedness.

5) National register of sovereign capabilities – ensuring visibility
A central register of Australian-owned providers should be established and maintained. This would give agencies a clear reference point in procurement and ensure local solutions are not overlooked. The register would not exclude international providers, but would ensure sovereign firms are considered first in line with Horizon 2's aim of systematising capability development.

6) Weighted evaluation criteria - recognising broader value
Tender evaluations should assign significant weighting to benefits such as workforce development, intellectual property retention, and sovereign industry growth, in addition to technical and cost factors. This is consistent with OECD recommendations on procurement that balances efficiency with long-term capability-building.

7) All-of-Government sovereign provider panel - ensuring consistency and scale
A standing panel of trusted Australian providers for critical cyber functions should be created. This would reduce reliance on ad hoc tenders that advantage incumbents and embed sovereign capability across the system, supporting Horizon 2's ambition to institutionalise resilience.

Thank you for the opportunity to contribute to this consultation. Australia already has a world-class cyber security industry. With the right support from government, these sovereign capabilities can scale further, creating jobs, retaining intellectual property, and ensuring that Australia invests in itself rather than in the capacity of others. Horizon 2 provides the opportunity to align procurement with strategy and secure the sovereign depth needed to protect our nation's security and economic interests.

Yours sincerely,

[redacted]

Department of Home Affairs
Australian Government
Discussion paper submission - Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Q39 (What role should government play in supporting the development and growth of Austalia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?

The OECD highlights that procurement should be used strategically to drive employment and skills outcomes, not simply to secure the lowest-cost supply. Governments that localise procurement are better positioned to strengthen domestic supplier capability, grow employment, and sustain industry skills (Implementing the OECD Recommendation on Public Procurement in OECD and Partner Countries).

When overseas providers are selected ahead of Australian businesses, local analysts and engineers lose access to the frontline delivery experience that builds capability. This weakens the workforce pipeline Horizon 2 seeks to expand and limits opportunities for Australian professionals to develop the expertise needed to meet emerging threats.

This is especially critical in fast-moving areas such as phishing and scam protection, where each contract represents a choice: to build Australia's sovereign workforce or to reinforce another country's capability at the expense of our own.

Australia has a strong cyber industry, built on highly capable professionals and competitive technology. Many firms and individuals deliberately remain in Australia, despite opportunities abroad, in order to contribute to national resilience. When long-term government contracts continue to flow offshore, the signal to these professionals is discouraging: investment in sovereign capability is not matched by policy practice. Over time, this risks eroding confidence and hollowing out the very sector Horizon 2 is designed to support.

Superficial remedies, such as staffing quotas or secondments, do not achieve deep skills development. When core delivery remains offshore, Australian personnel are confined to peripheral roles and miss the hands-on learning that comes only from being embedded in delivery teams and decision-making.

If high-value projects continue to flow overseas, Australia risks entrenching reliance on offshore providers whose decision-making and R&D sit outside our jurisdiction. This undermines resilience and slows the development of the next generation of Australian cyber leaders.

To support the development and growth of Australia's cyber workforce, government should:

Prioritise sovereign-led delivery in major contracts

1) Frontline cyber security delivery in critical areas should be led by Australian firms where they have proven capability.

2) This ensures local talent is exposed to complex challenges, building the skills pipeline, and advancing technology, rather than exporting it offshore.

Make workforce development a core delivery requirement

1) Where international providers are engaged, bids should be evaluated on how they embed Australian staff into meaningful delivery roles.

2) Points should be awarded for hands-on training, skill transfer, and pathways to long-term capability, not just token secondments.

Q39 (What role should government play in supporting the development and growth of Austalia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?

Recommendations continued...

Adopt dual-track procurement models

1) When an international incumbent is selected, where appropriate and practical, the next most qualified sovereign Australian firm should be contracted in parallel.

2) This allows government to retain continuity and global expertise while ensuring local providers gain real-world delivery experience that accelerates their growth and improves their global competitiveness.

Cap the length of foreign-only contracts at 24 months

1) Exclusive offshore agreements should be time-limited to prevent lock-in.

2) This creates recurring opportunities for sovereign providers to compete, demonstrate progress, and scale up their workforce capacity.

Establish a national register of sovereign cyber providers

1) A central register of qualified Australian firms should be maintained, including information on their workforce strengths and delivery history.

2) Agencies would be required to consult this register first when procuring services, ensuring sovereign firms are visible and considered on merit.

Measure and report workforce impacts of procurement

1) Agencies should publish how each major contract contributes to Australian jobs, skill development, and industry growth.

2) This transparency would hold procurement accountable for supporting the sovereign workforce pipeline, not just meeting short-term operational needs.

Department of Home Affairs
Australian Government
Discussion paper submission - Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Q44. How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?

Sovereign capabilities should be identified and prioritised through a structured national framework, rather than left to decentralised procurement processes. At present, capabilities are often "discovered" only when a tender arises, by which point established overseas incumbents already hold the advantage. A more deliberate approach is needed to ensure that Horizon 2 translates policy intent into practice.

Recommended Measures

Define priority sovereign service categories

1) Government should formally designate specific service areas where sovereign depth is essential to resilience, such as phishing and scam detection, takedown, DNS abuse enforcement, incident response, and threat intelligence.

2) Once defined, these categories would be subject to a "sovereign-first" procurement approach, ensuring Australian providers are considered before international options.

Conduct capability mapping with industry

1) Government should partner with local providers, industry bodies, and academia to map sovereign capacity: identifying which firms already deliver, which are emerging, and where capability gaps remain.

2) This creates a living picture of the sovereign ecosystem, helping agencies to plan procurement strategies that build depth rather than default to incumbents.

Establish a national register of sovereign providers

1) A central register should be created and maintained, listing Australian-owned firms that meet criteria such as onshore operations, IP retention, and proven capability.

2) Agencies would be required to consult the register before issuing tenders in priority categories, ensuring sovereign providers are considered on merit.

Prioritise through procurement weighting and constructive feedback

1) Tenders should assign weighting to sovereign capability, workforce development, and IP retention, not just cost.

2) Agencies should also be required to provide detailed, constructive feedback to unsuccessful local bidders. Currently, feedback is often cursory (e.g. brief debriefs despite significant bid effort). More robust feedback would allow sovereign firms to refine offerings and target R&D effectively.

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

Recommendations Continued...

Adopt dual-track procurement for international awards

1) When an international incumbent is engaged, where a locally qualified firm is identified, government should require a parallel sovereign contract in the same category.

2) This ensures local firms gain real-world delivery opportunities, build operational capacity, and refine their technology, while government benefits from continuity and global expertise.

Limit the length of foreign-only agreements

1) Where no sovereign capability exists and foreign providers are selected, contracts should be capped at 24 months.

2) Short-cycle contracts would prevent long-term lock-in, encourage competition, and give sovereign providers regular opportunities to compete as their capacity matures.

Outcome

Without such a framework, proven Australian solutions may continue to be overlooked, not because of capability gaps, but because there is no mechanism to recognise them as strategically important. By systematically defining, mapping, and prioritising sovereign services, Horizon 2 can ensure that domestic capability is developed alongside international partnerships, securing both national resilience and industry growth.