VeroGuard Submission to Horizon 2 Consultation

VeroGuard welcomes the opportunity to contribute to the Horizon 2 consultation of the Australian Cyber Security Strategy. As a sovereign Australian company delivering non-repudiable digital identity infrastructure, VeroGuard supports the Strategy's vision to make Australia a world leader in cyber security by 2030. This submission builds on our previous input to Horizon 1 and outlines how VeroGuard's technology and strategic approach align with the goals of Horizon 2.

Question 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?

VeroGuard Response: As a sovereign provider of non-repudiable digital identity infrastructure, VeroGuard recognises the importance of addressing this issue. Our platform offers secure hardware-backed authentication that is scalable across sectors. We recommend that Horizon 2 prioritise identity and access management reform, support sovereign technology adoption and incentivise strong authentication practices. This aligns with our previous submission and our commitment to enhancing Australia's cyber resilience.

The next few years will be defined by a seismic shift in the cyber threat landscape, driven largely by the proliferation of artificial intelligence (AI) and its application in offensive security. As highlighted in recent reports, AI models are now capable of autonomously discovering and exploiting previously unknown vulnerabilities at scale. Google's Project Zero and DeepMind collaboration, as well as platforms like XBOW, demonstrate that AI-powered bug hunting is no longer speculative - it is operational and effective. This marks the beginning of what could be described as an "armageddon of breaches", where the velocity and volume of exploit discovery far outpace traditional defensive capabilities.

This trend demands urgent strategic attention. The Government must anticipate and prepare for a future where AI-driven attacks are not only common, but devastatingly efficient. Horizon 2 must prioritise investment in AI-resilient infrastructure, automated patching systems and real-time threat intelligence sharing frameworks that can match the speed of AI adversaries.

Moreover, while phish-resistant multi-factor authentication (MFA) is becoming more mainstream, the reality is that the majority of businesses, websites and applications still do not support it. This leaves a vast attack surface vulnerable to credential-based attacks. The adage "hackers don't hack - they log in" encapsulates the core issue: existing authentication systems are fundamentally inadequate. The Government should both lead the way by demonstrating best practice and mandate or incentivise the adoption of hardware-based MFA across critical sectors, infrastructure and consumer platforms. This should be coupled with strong identity verification controls and continuous authentication mechanisms.

Strategically, Horizon 2 must also address the following:

- **Cyber Workforce Development**: AI will not replace human defenders but will augment them. Australia must invest in upskilling its cyber workforce to operate alongside AI tools, interpret AI-generated insights, and manage AI-driven defence systems.
- **Cyber Standards and Regulation**: Horizon 2 should establish enforceable standards for secure software development, AI safety in cybersecurity applications, and mandatory breach reporting.
- **Public-Private Collaboration**: Horizon 2 should deepen partnerships with industry to co-design scalable, interoperable cyber solutions, particularly in sectors like healthcare, finance, and critical infrastructure.
- **Resilience and Recovery**: As breaches become more frequent and severe, resilience planning - including cyber insurance, incident response capabilities, and national recovery frameworks - must be embedded into the strategy.

Horizon 2 must be bold and forward-looking. The convergence of AI and cybersecurity is not a distant future - it is today's reality. Without decisive action, Australia risks falling behind in a rapidly evolving threat environment. The Strategy must reflect this urgency and lead with innovation, regulation, and resilience. Critically, in Horizon 2 the Australian Government must also lead by example and build out Modern Defensible Architecture to act as an exemplar for industry.

Question 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?

One standout initiative is the Australian Cyber Collaboration Centre (A3C), based in South Australia. While technically a state-led program, the nature and impact of its work is national – and, increasingly, global - in scope. A3C exemplifies the kind of forward-thinking, capability-building infrastructure that should be replicated and scaled across other jurisdictions and integrated into federal strategy.

A key feature of A3C is its live-fire cyber range, which provides realistic, hands-on training environments for cyber professionals. This capability is not only rare in Australia but essential for preparing defenders to respond to real-world threats. A3C's involvement in the global Locked Shields exercise, the world's largest and most complex international live-fire cyber defence simulation, underscores its operational maturity and relevance. Participation in such events demonstrates that A3C is not just a training facility - it is a strategic asset contributing to national cyber resilience. Further, these activities should be expanded to also introduce Australian owned solutions and initiatives to drive and demonstrate local innovation in the cyber security industry.

Additionally, A3C offers structured training programs, industry collaboration opportunities and a platform for public-private partnerships. These elements are critical for developing a skilled cyber workforce and fostering innovation in defensive technologies. The Centre's model of combining education, simulation and collaboration should be adopted federally and by other states and territories.

To strengthen Australia's cyber posture under Horizon 2, the Government should:

- Expand live-fire cyber ranges nationally, modelled on A3C's infrastructure and curriculum;
- Fund and support cross-jurisdictional participation in global cyber defence exercises like Locked Shields;
- Integrate A3C-style training into national cyber workforce development plans, ensuring consistency and excellence across the country; and
- Establish a federated network of cyber collaboration centres, enabling knowledge sharing, joint exercises, and coordinated incident response.

In summary, A3C is a blueprint for what effective, scalable, cyber capability development looks like. Its replication and integration into federal strategy would significantly enhance Australia's readiness for the evolving threat landscape.

Question 3 Does the high-level Model resonate and do you have any suggestions for its refinement?

The **Cyber Security Policy Evaluation Model** presented in Figure 5 of the Horizon 2 paper is a commendable attempt to provide a structured framework for assessing policy effectiveness. However, to enhance its utility and localisation, we offer the suggestions below.

The Model uses terms like "interventions," "North Stars" and "causal hypotheses." Replacing these with plain-language labels **such as "**What We Do**", "**Goal**"** and **"**Expected Result**" will make this more useable for the general public to enable them to grasp** the Model more quickly, create more purpose behind the Model and activate a sense of urgency to act.

We also request that local language/terminology is maintained. Use of terms like **North Star** suggest this is not Australian or that we only look towards the Northern Hemisphere for best practice and solutions. North Star is not a term we use in Australia and we cannot even see the North Star!

The Model also feels linear and appears to suggest that the only driver for a new cycle is the adoption of new technology. Cybersecurity is dynamic and the inclusion of feedback loops to represent learning, where outcomes feed back into refining interventions, would make the Model appear iterative rather than linear.

Shield 1: Strong businesses and citizens

Question 4 Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?

We believe that government has already established appropriate measures and information gathering mechanisms. The primary focus must be on taking actions for greater resilience. The Frameworks started by ASD for Modern Defensible Architecture are a good example of where priorities should be made.

Question 5 What could government do to better target and consolidate its cyber awareness message?

Government has done a lot of positive work in building out models, tools, information and public awareness campaigns. Horizon 2 should be about prioritising building cyber security infrastructure and uplifting local capability (people and solutions).

Question 6 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?

Government has successfully developed many programs including: Cyber.gov.au, ASD Advisory's, Essential eight, ASD | DFIR Fortnightly Operational Snapshot and the ACSC Partnership Program.

We believe that the area of greatest focus moving forward to uplift capability should be to embrace collaboration with Australian cyber security companies and experts to more emulate programs in world leading cyber countries. Examples include Estonia, Finland, Israel the US and UK.

Question 7. How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?

Outside existing initiatives that encourage and promote improved cyber resilience, Government should be establishing minimum criteria for tendering to Government at federal and state levels to meet Essential 8 compliance driving more organisations to seek out the resources. As an example, the organisational profile in the Consolidated Tenders platform enables an organisation to provide a snapshot of their current E8 rating which can be then used to preselect suitable organisations for invitation into closed tenders. Leveraging this type of structure more widely would further encourage SMEs to seek out and uptake available resources.

Question 8 How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?

See response to Q7.

Question 9. What existing or developing cyber security standards could be used to assist cyber uplift for SMBs and NFPs?

No response.

Question 10. 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 in the NFP sector?

No response.

Question 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 is increasingly recognised as essential for Australian SMEs, but affordability and accessibility remain significant barriers. Small businesses - especially those with limited cybersecurity maturity – lack the knowledge to understand the perceived complexity of policies and coverage terms. Further, for the same reason, they lack the internal cyber skills to protect themselves and therefore reduce their cyber exposure that would lead to lower premiums.

To address these challenges, government-backed initiatives to support SME access to cyber insurance could include subsidised premiums, simplified certification frameworks and incentives for adopting baseline cybersecurity controls. Such measures would not only improve SME resilience, but also reduce systemic risk across the broader economy.

Question 12. How well do you consider you understand the threat of ransomware, particularly for individuals and small entities?

No response.

Question 13. How could the government further support businesses and individuals to protect themselves from ransomware attacks??

See response to Q7

Question 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?

No response.

Question 15. How can support services for victims of identity crime be designed to be more effective in the context of increasing demand? How can technology be used to support individuals in managing and recovering from identity crime?

Whilst services, like IDCare, do fantastic work and will need continued increased funding (perhaps funded by fines for corporate breaches), much more effort needs to be put into prevention rather than cures. For example, robust digital identity like other leading countries.

Question 16. Which regulations do you consider most important in reducing overall cyber risk in Australia?

Australia has made significant strides in cybersecurity regulation, especially with the recent introduction of the **Cyber Security Act 2024**, which is part of a broader push to make the country a global leader in cyber resilience by 2030.

This legislation introduced four major reforms:

- **Minimum Security Standards for Smart Devices**
  Manufacturers must meet baseline cybersecurity requirements for connected products like smart watches and baby monitors.
- **Mandatory Ransomware Reporting**
  Certain businesses are now required to report ransomware incidents, helping authorities understand the scale and nature of attacks.
- **Limited Use Obligation**
  Ensures information shared during cyber incidents is not used for civil or regulatory action, encouraging transparency and cooperation.
- **Cyber Incident Review Board**

  Conducts independent, no-fault, reviews of major incidents to improve future prevention and response strategies.

Further work can be done:

- Building cyber security compliance requirements for Government tenders.
- Administering actual fines for breaches
- Assessing the applicability of the UK banking cyber regulations
- Further upgrades and penalties for SOCI

The Privacy Act regulates how personal data is handled, especially by entities covered under the Australian Privacy Principles – however, more could be done to remove some requirements for the collection and storage of PII by every service organisation through the introduction of a centralised federated digital identity.

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

Yes, while cybersecurity compliance in Australia is essential for national resilience, it can lead to **unintended negative outcomes** for some organisations—especially when compliance is treated as a box-ticking exercise rather than a strategic investment.

Cybersecurity Compliance can cause resource strain, as SME's and local agencies often lack the budget, expertise or infrastructure to meet complex compliance requirements, which can lead to **diverted resources** from core operations or innovation, especially when compliance frameworks are rigid or poorly tailored.

Compliance Fatigue. Constant updates to regulations and reporting obligations can overwhelm teams, leading to burnout or disengagement.

False Sense of Security. Meeting compliance standards does not always mean an organisation is secure. Over-reliance on compliance checklists can mask **real vulnerabilities**, especially in dynamic threat environments.

Reputational Risk from Mandatory reporting. Mandatory ransomware reporting, while beneficial for national threat intelligence, may expose organisations to **public scrutiny** or **loss of trust**, especially if incident details are leaked or misunderstood.

Potential considerations to mitigate these issues

- **Tailoring compliance models to** sector-specific frameworks that scale with organisational size and risk profile.
- **Cyber uplift grants**: Offer financial and technical support to SMEs and regional agencies to meet standards without compromising operations.

Shield 2: Safe technology

Question 18. What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?

Critical Infrastructure OT - Energy, Water, Transport

These sectors face an escalating cyber threat landscape, with a surge in ransomware attacks, state-sponsored intrusions and vulnerabilities in operational technology (OT) systems. Credential and identity compromise remains the leading cause of breaches, being involved in over 90% of incidents. Despite the growing adoption of Zero Trust principles, very few organisations have fully implemented them, largely due to legacy infrastructure and complexity. Traditional IT security practices are insufficient for OT environments, where patching is often impractical and air-gapping can hinder operational efficiency. The need for robust, scalable, identity-centric solutions is urgent.

To strengthen Horizon 2, the Government should consider improved cyber infrastructure and compliance so that standards reflect actual available capabilities and not accept the compromises that may exist today in critical infrastructure. Like many best practice nations, the Australian Government should be supporting scalable sovereign capabilities for securing critical infrastructure. Benefits would include uplifts to local capability, improved cyber infrastructure, improved efficiency and effectiveness and significant net overall economic outcomes. By embedding identity at the core of cyber strategy, Australia can better defend its broader critical infrastructure against emerging threats.

Question 19. How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?

World leading countries, such as Estonia, focus on building cyber infrastructure and local capability by partnering with sovereign companies as their priority. Lifting awareness and knowledge then flows from that point.

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

To strengthen Horizon 2, the Government should also seek to define and communicate component sourcing policies.

As the geopolitical environment is evolving rapidly, government should ensure sovereign capability is viable and sustainable through early and clear guidance regarding the sourcing of components and compliance. Redesigning products, reworking production lines and requalifying firmware to meet shifting procurement standards is a time and cost-intensive process. Without timely direction, Australian innovators risk being excluded from government procurement pipelines due to misalignment with evolving policy.

Should this risk materialise, Australia's ambition to lead in cybersecurity could be significantly undermined. Without proactive engagement and support, Australian companies may find themselves blocked from participating in the very initiatives designed to strengthen national cyber resilience.

This would increase reliance on foreign technologies, potentially exposing critical infrastructure to supply chain vulnerabilities and geopolitical risk.

To avoid this, Horizon 2 must include a clear framework for sovereign capability development, including early-stage guidance on approved sourcing, certification pathways and procurement alignment. Doing so will ensure that Australian cybersecurity providers can contribute meaningfully to national security objectives, while fostering local industry, innovation and jobs growth

.Question 21. How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?

Identify and trial sovereign capability to inform decisions and uplift local capability in line with world leading nations in this area.

Question 22. Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How does Government and Industry work together to achieve this aim in an evolving global threat environment?

- See response to Q21
- Build more robust cyber infrastructure, particularly in the area of identity.

Question 23. What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies? What do you consider to be the most serious national security risks presented by critical and emerging technologies, such as AI?

See response to Q1, where we raise the concerns of AI and the pending tsunami of vulnerabilities heading our way.

Shield 3: World-class threat sharing and blocking

Question 24. What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry? Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry?

We recommend that Horizon 2 prioritise identity and access management reform, support sovereign technology adoption and incentivise strong authentication practices. This aligns with our previous submission and our commitment to enhancing Australia's cyber resilience.

The adage "hackers don't hack - they log in" encapsulates the core issue: existing authentication systems are fundamentally inadequate. The Government should mandate or incentivise the adoption of hardware-based MFA across critical sectors, infrastructure and consumer platforms. This should be coupled with strong identity verification controls and continuous authentication mechanisms.

The Government needs to scope and define what proactive cyber security posture looks like.

An excellent start in this has already been made with the Modern Defensible Architecture Framework by ASD, which is shaping up to provide the guidance needed. However, empowerment will come from not just establishing the frameworks, but also by identifying and demonstrating best practice in Government as the exemplar that itself utilises sovereign capabilities. This will encourage an uplift in capability which will then spill over into industry. This has been proven in countries like Estonia, Israel and Finland.

On a specific point, while phish-resistant multi-factor authentication (MFA) is becoming more mainstream, the reality is that many businesses, websites and applications still do not support it. This leaves a vast attack surface vulnerable to credential-based attacks and, with the growing sophistication of AI and its capability to enhance social engineering, we are likely to see that anything less that hardware base MFA will be easily bypassed at scale.

Sector Responses

General

VeroGuard is a sovereign digital identity vendor. We developed our non-repudiable digital identity infrastructure because we believe that identity is the new frontier for cyber defence and a strong identity posture goes a long way to protecting against the majority of cyberattacks. Business continues to put systems and networks onto the internet and then relies on identity to solve the security problem, yet many organisations have not addressed even the most basic of password hygiene requirements. Attackers have worked out that it is far easier to trick a user into divulging information than actually breaking into systems through vulnerabilities and other sophisticated attacks. Once they have your credentials, there are no conditional access policies that can totally protect your environment.

The bottom line is that, even if we fixed every software problem, removed every memory corruption, eliminated programming flaws and buffer overflows and have the best detection and response systems, **we still a need robust and functional identity.** For this reason, we created the VeroGuard Platform and believe that every sector could benefit from a robust identity solution.

VeroGuard also has insight into a number of sectors called out in the consultation and offers our insights on each below.

health

The Australian healthcare sector is undergoing rapid digital transformation, driven by the adoption of technologies such as IoT, AI and cloud-based systems. However, this evolution has significantly expanded the attack surface, with identity compromise remaining the leading cause of breaches. The complexity of legacy systems, hybrid environments and fragmented identity and access management frameworks has made healthcare infrastructure increasingly vulnerable. VeroGuard highlights that the next generation of health systems must be designed with identity and data security at their core, leveraging unified platforms and hardware-based security to ensure resilience and privacy.

VeroGuard's sovereign platform offers a scalable, defence-certified, solution that applies military-grade HSM-to-HSM encryption to both human and machine identities. This architecture enables secure access to medical systems, records and devices, while simplifying integration across supply chains, staff and patient ecosystems. Supporting the adoption of sovereign technologies like VeroGuard can strengthen national capability and position Australia as a global leader in cyber-secure digital health. Sponsoring the deployment of such platforms will accelerate transformation while ensuring uncompromised security and privacy for all stakeholders.

research and academia

Australia's research and academic institutions are often working at the forefront of global innovation, in highly sensitive and cutting-edge domains such as quantum computing, biotechnology, defence technologies and artificial intelligence. However, this leadership position also makes them prime targets for cyber espionage and intellectual property (IP) theft. State-sponsored actors and sophisticated cybercriminals are increasingly targeting universities and research centres to exfiltrate valuable data, disrupt operations or gain strategic advantage. The loss of IP not only undermines national competitiveness, but also erodes trust in Australia's research ecosystem.

Securing these environments is uniquely challenging. Research networks are inherently open and collaborative, often involving international partners, decentralised infrastructure and a mix of legacy and experimental systems. Traditional security models struggle to keep pace with the dynamic and decentralised nature of academic environments. The adoption of **Next Generation Authentication (NGA)** - such as VeroGuard's sovereign, hardware-based, identity platform - can provide a critical layer of protection. By ensuring irrefutable identity verification for both users and machines, NGA can prevent credential compromise, secure remote access and protect sensitive research data across hybrid and open networks.

To support Horizon 2's goals of global leadership and sovereign capability, the Government should prioritise investment in secure digital identity infrastructure for the research sector. This includes

sponsoring the adoption of sovereign cybersecurity technologies by universities and research institutions, particularly those engaged in critical or export-sensitive fields. Doing so will not only protect Australia's intellectual capital, but also foster a secure, trusted environment for innovation and international collaboration.

financial services sector

The banking and financial services sector remains a prime target for cybercriminals due to the high value of financial data and transactions. The increasing sophistication of threats - particularly those powered by AI - has exposed the limitations of traditional cybersecurity measures, including conventional multi-factor authentication (MFA). Attackers are now bypassing these defences through credential theft, phishing and social engineering, leading to what is described as the "industrialisation of cybercrime". The sector also faces challenges integrating modern security into legacy systems, managing insider threats and dealing with alert fatigue in security operations centres.

To address these challenges, the government should mandate the phased adoption of **Next Generation Authentication (NGA) -** phish-resistant, hardware-based, identity verification solutions within the financial sector, to protect customer accounts from malicious credential-based attacks. The VeroGuard Platform, developed by an Australian sovereign cybersecurity company, offers a defence-certified solution that uses Hardware Security Modules (HSMs) to create secure, encrypted and verifiable identity authentication over open networks. This approach eliminates credential compromise, simplifies access management and supports Zero Trust architectures. It is scalable across legacy, cloud and hybrid environments, and can be deployed cost-effectively without major infrastructure changes.

Supporting sovereign technologies like VeroGuard not only enhances national cyber resilience, but also aligns with Horizon 2's goals of fostering global leadership and economic growth. By sponsoring adoption of such platforms, the Government can help reduce systemic risk, protect critical financial infrastructure and create high-value jobs in the cybersecurity sector.

As a sovereign provider of non-repudiable digital identity infrastructure, VeroGuard recognises the critical importance of reforming identity and access management across Australia's cyber landscape. Our platform delivers secure hardware-backed authentication that is scalable across sectors and purpose-built for open networks. We strongly recommend that Horizon 2 prioritise identity-centric security architecture as a foundational element of national cyber resilience.

Supporting sovereign cybersecurity providers like VeroGuard also not only strengthens Australia's digital defences, but also contributes directly to domestic job creation, skills development and economic growth. By sponsoring the adoption of sovereign technologies - particularly among SMEs - the Government can accelerate innovation, reduce reliance on foreign solutions and position Australia as a global leader in cybersecurity. This aligns with Horizon 2's ambition to build a secure and prosperous digital future, and with our ongoing commitment to enhancing Australia's cyber resilience through scalable, high-assurance infrastructure.

Question 25. Does the government need to provide clarity on permissible and non-permissible Active Cyber Defence in the Australian context?

Yes.

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

- Act as an exemplar
- Build improved cyber infrastructure
- Build robust digital identity

Question 27. How could the use of safe browsing and deceptive warning pages be amplified?

No response

Question 28. What more is needed to support a thriving threat sharing ecosystem in Australia?. Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?

Greater investment in the National Cyber Security Co-Ordinator's Group.

Question 29. Question 14. How can we better align and operationalise intelligence sharing for cyber security and scams prevention?

See response to Q28

Question 30. 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?

See response to Q2, with respect to growing the capability provided by A3C across all government's layers and levels. Experience in a live-fire situation is invaluable and should be a pre-requisite for senior Security roles within government and larger organisations.

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

Unfortunately, this may only be achieved through escalating fines for delays in compliance.

Question 32. Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?

Yes

Shield 4: Protected critical infrastructure

Question 33 How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?

See below

Question 34. Are there significant cyber security risks that are not adequately addressed under the current framework?

See below

Question 35. Is the regulatory burden on industry proportionate to the risk and outcomes being sought?

See below

Question 36. What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?

The Security of Critical Infrastructure (SOCI) Act plays a vital role in safeguarding Australia's essential systems and services. The recent amendments have significantly improved clarity, consistency and coordination across sectors, particularly in the face of escalating cyber threats. VeroGuard supports the direction of these reforms, especially the move away from voluntary compliance toward enforceable standards.

In our previous submission, we noted that the increasing integration of IT and OT systems, combined with exposure to open networks and cloud environments, demands a more robust and mandatory framework.

However, for the SOCI Act to be truly effective, it must go beyond policy and enforcement—it must also support the practical implementation of sovereign cybersecurity capabilities.

To ensure the SOCI Act continues to protect Australia's infrastructure effectively, we recommend that Horizon 2 include provisions for:

- **Stronger regulatory requirements** for critical infrastructure operators, moving beyond voluntary compliance.
- **Improved clarity, consistency, and coordination** across sectors to ensure a unified national approach to cyber resilience.
- **Mandatory standards and advisories** for cybersecurity technologies applied to critical infrastructure, similar to binding directives issued by agencies like CISA, NIST and NSA in the United States.

- **Support for integrated IT/OT environments**, recognising the increasing exposure of operational technology to open networks and cloud services.

This approach will not only enhance enforceability and understanding of obligations, but also foster a resilient sovereign cybersecurity ecosystem capable of defending Australia's critical infrastructure in an increasingly hostile digital landscape.

Question 37. How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?

- See response to Q36

Question 38. How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?

There are certain areas where security requirements have driven compliance when building infrastructure specifically for Government, however it has not flowed down yet to other industries. Government can note, however, that organisations do comply where standards are mandated when engaging with Government.

Shield 5: Sovereign capabilities

Question 39. What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?

Government's role should include significantly greater collaboration and adoption of sovereign solutions. All world leading cyber security countries have programs that are specifically focused on sovereign capability. The most significant impact comes from having real world programs in government utilising sovereign solutions where all parties learn and develop that capability in the real-world environment. This can easily be activated by supporting and funding CIO's and CISO's to run sovereign only pilots to address specific problems. This approach has been adopted by and continuously run by leading cyber countries, irrelevant of their country size.

Question 40. What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?

No response

Question 41. What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?

Whilst we are not experts in this area, VeroGuard can be used as an example of a domestic organisation that has re-skilled ex-automotive workers in South Australia to be part of its advanced manufacturing of the VeroGuard Platform.

Question 42. How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals?

See response to Q39.

Question 43. How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities?

See response to Q39 and then link in academia with the sovereign capability. By working together on real world problems, the focus improves, capability lifts and we get greater efficiency in the system.

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

See response to Q39. Further, to strengthen Horizon 2, the Government should prioritise platforms and systems that have been certified for high assurance environments and remove the red tape on Agencies needing to re-prosecute these systems for security attestation.

Question 45. What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?

Australia's current ICT concentration is a significant risk to building capability and new generation industries. Australia must build a strong incubation and innovation environment for sovereign technology to avoid becoming just a branch office to other countries. It is critical that Government leads the way in initiatives to build and support sovereign solutions. This has already been successfully demonstrated in leading cyber security countries around the world.

Shield 6: Strong region and global leadership

Question 46. Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?

No response

Question 47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

Australia must build and grow its own capability that it can share and promote with our neighbours.

Question 48. Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?

By adopting better engagement with sovereign organisations, Cyber RAPID, in collaboration with Australian companies, could improve those nations capabilities. Happy to expand on this idea.

Question 49. In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?

We believe that building resilient infrastructure is the highest priority and therefore engaging industry on the next iterations of Modern Defensible Architecture and maintaining a balanced mix of organisations participating in other cyber industry forums will yield the best results.

Question 50. What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?

As a priority, Australia should continue to align with the US, UK and European cyber frameworks and standards.