[redacted]
www.bdo.com.au

[redacted]

Cyber Security Strategy Team
Department of Home Affairs
homeaffairs.gov.au

Re: Submission to Horizon 2 Consultation - 2023-2030 Australian Cyber Security Strategy

BDO Australia is pleased to submit our response to the Department of Home Affairs' consultation on Horizon 2 of the 2023–2030 Australian Cyber Security Strategy.

Our response draws on insights from BDO Australia's cyber security, risk advisory, and digital transformation teams. We have placed particular emphasis on the needs of small and medium businesses (SMBs), not-for-profits (NFPs), and critical infrastructure operators — groups that face unique challenges but are central to strengthening Australia's national resilience.

Our submission includes practical recommendations to:

- Uplift national cyber resilience through scalable certification models and trusted labelling schemes
- Improve supply chain security and data governance frameworks
- Enhance consumer protections and trust for emerging technologies such as AI
- Promote a proactive national cyber posture that balances prevention, response, and recovery
- Foster deeper collaboration between government, industry, and regulators to accelerate secure technology adoption and trusted data sharing across the economy.

We commend the Department's inclusive and forward-looking approach to this consultation and welcome the opportunity to continue contributing to this important national effort.

Yours sincerely,

[redacted]
Partner and National Cyber Leader

[redacted]
Partner and Federal Government Cyber Leader

2023-2030 Australian Cyber Security Strategy

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?

Australia's cyber outlook over the next few years will be shaped by rapid advances in AI, quantum technologies, data-driven systems, and digital transformation. These technologies will unlock opportunity but also create systemic vulnerabilities that government and industry must plan for.

- Generative and agentic AI adoption: AI will accelerate both cyber threats (e.g., AI-driven phishing, deepfakes, automated vulnerability discovery) and national dependencies, as AI becomes embedded in critical business processes. Once in place, AI systems will be core to operations, raising the resilience question: how do organisations cope if AI systems fail, are corrupted, or manipulated? Government should develop guidance for AI resilience and recovery, akin to disaster recovery planning for IT.
- AI as core intellectual property (IP): Models, algorithms, and training datasets will increasingly define competitive advantage, making them high-value targets. Protecting this AI "IP" from theft, manipulation, or exfiltration will be essential for both national security and economic growth. This may require new IP protection frameworks, stronger trade secret enforcement, and incentives for secure-by-design AI practices.
- Quantum-powered AI: The convergence of quantum computing with AI will supercharge these dynamics. Quantum-enhanced AI will enable faster, more powerful analysis and optimisation, but will also magnify risks by accelerating threat modelling, cryptographic breaking, and attack automation. In a quantum-powered AI future, everything becomes "bigger, faster, and more powerful" — requiring government to invest now in post-quantum cryptography, AI model assurance, and scenario planning for quantum-AI enabled attacks and defences.
- Data quality and governance challenges: Poorly managed, siloed, or unstructured data will continue to constrain safe AI use while increasing risks of breaches and insider misuse. National frameworks on data classification, governance, and secure pipelines will be critical to harnessing AI safely.
- Expanding attack surfaces: The growth of cloud, IoT, 5G, and hybrid work has permanently broadened the attack surface. These interconnected environments require stronger baseline standards and supply chain assurance mechanisms, especially where AI is deployed at the edge.
- Privacy and digital trust expectations: Rising regulatory and consumer expectations will mean trust becomes a market differentiator. SMBs and NFPs in particular will need government support to implement privacy-by-design and Essential 8 maturity roadmaps.

In summary, Government should explore the following strategic factors under Horizon 2:

- Develop national AI resilience and recovery guidance
- Treat AI models and data as protected IP, with updated frameworks
- Prepare for post-quantum cryptography and plan for how quantum-powered AI could be used in future cyber-attacks and defences
- Work with industry to strengthen/develop sector-specific data governance frameworks
- Mandate supply chain security standards for AI/IoT/cloud vendors

- Support privacy-by-design as a competitive advantage for Australian businesses.
- Global example:
    - Government should look at how the EU's AI Act regulates high-risk AI as critical technology, while the US and NIST are preparing for a quantum future through post-quantum cryptography standards. Australia should bring both of these approaches together in Horizon 2.

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?

Several State and Territory governments have piloted effective initiatives that could be scaled nationally. For example, the Queensland Government's Cyber Security Unit provides guidance and shared resources to uplift cyber maturity, while the Business Basics and Business Growth Fund grants include support for digital and cyber security investment for SMBs. Similarly, the NSW Cyber Security Policy and services delivered by Cyber Security NSW show the benefits of centralised expertise and shared services for agencies, councils, and smaller organisations. Some States have also piloted cyber awareness programs in schools, embedding digital safety and resilience into the curriculum at an early stage.

While these programs are valuable, more can be done to communicate them effectively to industry associations, chambers of commerce, and NFP networks, so SMBs and NFPs are fully aware of the support available. Replicating and expanding these initiatives nationally—particularly through consistent grant programs, shared services, and education campaigns—would create stronger national baselines and ensure equitable access to cyber resilience support across all sectors. Internationally, models such as the UK's NCSC Small Business Guide and Cyber Essentials certification and Singapore's Cybersecurity Grant for SMBs demonstrate how government-led programs, paired with strong industry engagement, can accelerate uplift and provide practical, affordable pathways for smaller organisations.

2.3 Monitoring progress in a changing world – a conceptual framework for evaluating cyber security outcomes

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

Yes, the high-level Model resonates in mapping interventions to outcomes and using "North Stars" as guiding objectives. However, refinement is needed to ensure the Model balances likelihood reduction (prevention) with impact management (response and recovery), which are equally important for SMBs and NFPs that often face existential risks from incidents. The Model should also explicitly incorporate education and awareness outcomes (e.g., cyber literacy in schools), supply chain resilience, and the adoption of accessible industry certification schemes such as SMB1001, CyberCert, and global equivalents like Cyber Essentials. Finally, the Model should track not just risk reduction, but also positive benefits of uplift such as customer trust, brand reputation, improved market access, and reduced insurance costs.

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

Monitoring should be multi-layered, drawing on quantitative data (e.g., cyber incident reporting trends, uptake of Essential 8 maturity levels, certifications like CyberCert/SMB1001, insurance product adoption) and qualitative insights (e.g., SMB/NFP surveys on barriers, case studies on the impact of ransomware, community consultations). Existing platforms such as the ACSC threat-sharing network and the Mandatory Data Breach Notification scheme could be extended to feed into outcome monitoring. New approaches could include:

- Partnering with insurers and banks to collect anonymised data on uptake of baseline controls linked to finance and insurance access
- Using regulatory touchpoints (ASIC, ACNC, ATO portals) to embed lightweight self-assessment check-ins
- Establishing a national dashboard with traffic-light ratings for cyber maturity across SMB, NFP, and sectoral cohorts to make progress transparent.

Shield-level focus for Horizon 2

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

The government has invested heavily in cyber awareness material, but it is often fragmented and difficult to locate. A more effective approach would be to centralise resources in a single trusted portal and push awareness through regular touchpoints such as annual tax returns, Medicare, or banking services. Embedding cyber education into school curricula will also strengthen resilience from an early age.

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 should strengthen cyber education by embedding awareness in schools and through regular citizen touchpoints such as tax returns and Medicare services. Industry-led initiatives like SMB1001 and Cyber Wardens have shown promise in raising awareness and practical capability, but greater support and scaling is needed. Further progress can be made by incentivising partnerships between government, industry, and vendors to deliver cost-effective, Essential 8–aligned training and tools that are easy for SMBs and NFPs to adopt.

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.)?

Government can increase uptake by integrating cyber resources into existing regulatory and service interactions, such as ASIC, ACNC, or ATO portals, where SMBs and NFPs already engage. Industry-led initiatives like SMB1001 and CyberCert should be promoted alongside government programs, as they provide practical, scalable pathways to uplift capability. A certification model, similar to the “Energy Star” rating, would incentivise organisations to demonstrate baseline security maturity, and linking this to tangible benefits such as lower cyber insurance premiums or procurement eligibility would further drive adoption.

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?**

Partnerships between industry, government, and insurers should focus on offering bundled, cost-effective solutions that align with the Essential 8. Industry-led initiatives such as SMB1001 and CyberCert provide proven models for practical uplift and should be expanded nationally with government support. Industry associations can also play a stronger role by sharing real-world impact stories of cyber incidents to encourage uptake, while government can co-fund pilots and promote trusted vendor marketplaces to scale adoption.

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

The Essential 8 framework provides a strong baseline, but many SMBs struggle with implementation. Industry-led initiatives such as SMB1001 and CyberCert, alongside global examples like the UK's Cyber Essentials and the US NIST Cybersecurity Framework for Small Businesses, demonstrate that practical certification models can make cyber standards more accessible and scalable for smaller organisations.

Government could build on these by:

- Developing a certification scheme similar to "Energy Star" that recognises incremental maturity and is easy for SMB's and NFP's to adopt
- Exploring an "ACSC approved build" for ubiquitous technologies (e.g. common operating systems, email platforms, and cloud tools), giving smaller organisations a practical, pre-hardened option that reduces configuration risk
- Raising awareness of privacy regulations through simplified compliance guidance, helping businesses strengthen trust while reducing risk exposure.

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?**

NFPs often operate with limited budgets and rely heavily on volunteers, making it difficult to prioritise cyber security investment. While sector-specific tools such as the ACSC's Cyber Wardens program, ACNC's cyber governance guidance, and discounted security offerings from global providers like Microsoft and Google for charities have been developed, awareness and uptake remain limited.

Government could increase visibility of these resources and introduce incentives—such as payroll tax reductions for vendors and consultancies that subsidise or donate cyber services to NFPs—to expand affordable access to Essential 8–compliant tools, identity monitoring, and tailored sector guidance.

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 at times be unaffordable for SMBs and NFPs, with premiums potentially exceeding what these organisations can allocate. Policies are complex, and insurers often require security measures that small entities struggle to evidence. Uptake could be improved by aligning insurance with accessible certification schemes such as SMB1001, CyberCert and offering bundled solutions that include affordable tools like Microsoft Defender for Business, CrowdStrike Falcon Go, or managed back-up and identity monitoring services. These bundles would not only lower the barrier to entry but also provide insurers with assurance of baseline controls, helping reduce premiums and broaden accessibility.

12. How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?

Ransomware remains one of the most pressing threats, with attackers increasingly targeting SMBs and NFPs due to weaker defences, reliance on third parties, and the growing use of double extortion tactics. A likely next evolution of ransomware attacks will be 'AI-informed ransomware', where attackers use AI to study user behaviour and target those most likely to fall for scams. This makes attacks more personalised, harder to spot, and more damaging.

Public understanding is still too often shaped by regulatory penalties, rather than the real-world impact on victims. Greater emphasis should be placed on sharing stories from impacted organisations, particularly SMBs, about operational disruption, financial strain, and reputational damage, as these experiences drive more practical awareness and behavioural change.

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

Support should focus on both prevention and recovery. Beyond providing protective tools, government could subsidise affordable identity monitoring, back-up solutions, and incident response training tailored for small entities. Partnerships with vendors and insurers to deliver cost-effective, Essential 8-aligned bundles would also strengthen resilience. Importantly, education and awareness campaigns should not only highlight what can go wrong but also emphasise the benefits of stronger security—such as improved customer trust, reduced downtime, and better access to finance and insurance—to create positive drivers for adoption.

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?

SMBs and NFPs are disproportionately impacted by cyber incidents due to limited resources, lack of in-house expertise, and reliance on third-party services. Common vulnerabilities include weak back-up practices, poor patching, limited monitoring, and general lack of awareness of cyber, data, and privacy risks. The impacts extend beyond financial loss to service disruption, reputational damage, and loss of donor or customer trust, which can be existential for smaller organisations. For NFPs, significant effort and resources are often redirected toward managing the fallout of incidents rather than delivering their core charitable services. Taking a proactive approach to cyber resilience would allow NFPs to better focus their resources on their primary mission of serving the community.

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

Support services need to be simple, affordable, and accessible to individuals, SMBs, and NFPs. A centralised government-backed identity monitoring service—delivered in partnership with banks, insurers and medical aid providers —would provide a trusted "one-stop shop" for victims. Incentives such as subsidised or free access for smaller organisations, coupled with clear pathways for reporting, recovery, and education, would ensure victims can quickly mitigate harm while improving overall awareness of identity risks.

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

Privacy regulations play a key role in reducing cyber risk by requiring better data management and accountability. For SMBs, awareness should focus not only on regulatory penalties but also on the real impact of non-compliance, including loss of customer trust and loyalty, which often carries greater

long-term consequences. Introducing a privacy compliance certification—similar to the "Energy Star" rating—would provide a clear, visible marker of trustworthiness, making compliance obligations more practical and improving customer confidence. Clearer alignment between regulatory requirements and frameworks such as the Essential 8 would further support uplift and reduce compliance complexity.

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

As a professional services organisation, regulatory and compliance requirements have generally had a positive impact on our cyber maturity. They have assisted us to strengthen governance, improve alignment to frameworks such as the Essential 8, ISO 27001, etc. and build more robust processes for incident management, data protection, and client assurance. For our firm, these obligations act as a catalyst to continuously improve, rather than a barrier.

At the same time, through our work with SMBs and NFPs, we see the other side of the challenge. For smaller entities, compliance obligations often create significant administrative overhead when they lack dedicated cyber or risk resources. This sometimes leads to a "tick-box" approach rather than genuine risk reduction. Streamlining requirements, providing sector-specific guidance, and aligning obligations with practical frameworks like the Essential 8 would reduce the burden while still improving maturity. At the same time, it is important to highlight that compliance can strengthen branding and customer trust, which are powerful drivers for SMBs and NFPs to invest in better security and demonstrate accountability.

3.2 Shield 2: Safe technology

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?

- Consumer / Edge Devices: The UK's Product Security and Telecommunications Infrastructure (PSTI) Act mandates unique passwords, clear support periods, and vulnerability disclosure policies for connected devices, complemented by a voluntary Cybersecurity Labelling Scheme in Singapore. These models could be applied to smart home and healthcare devices in Australia
- Consumer Energy Resources (CER): The California Public Utilities Commission has embedded security requirements into DER (Distributed Energy Resources) interconnection rules using IEEE 1547. In the EU, IEC 62351 is being used to secure communication between solar inverters, EV chargers, and grid operators. These examples could inform standards for Australia's rooftop solar, smart inverters, and home batteries
- Operational Technology (OT): The US NIST SP 800-82 and IEC 62443 standards are widely adopted in the energy and manufacturing sectors to secure SCADA and ICS environments. For example, the European Network for Cyber Security (ENCS) applies IEC 62443 to protect electricity distribution networks.

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?

Government can play a stronger role in shaping consumer cyber awareness by embedding governance mechanisms and working through trusted industry channels:

- Certification and labelling: Expand industry programs like CyberCert or SMB1001, modelled on the UK's Cyber Essentials, to provide an easily recognisable certification for products and services. This would give consumers the confidence that baseline controls (e.g., MFA, encryption, update support) are in place and encourage vendors to compete on security, not just price.
- Cyber "fact labels" on devices: Similar to the Australian Energy Regulator's Better Bills Guideline, require plain-English, standardised labels on IoT and smart devices at point-of-sale. International examples such as Singapore's Cybersecurity Labelling Scheme and the US "Cyber Trust Mark" show how labels can display update policies, vulnerability reporting processes, and security support periods to help consumers make informed choices.
- Targeted awareness through trusted channels: Partner with retailers (e.g., JB Hi-Fi, Officeworks, Harvey Norman) to display consumer-friendly cyber checklists, and with banks (e.g., CBA's "Safe and Savvy" program, NAB's cyber safety outreach) to deliver tailored campaigns for vulnerable groups such as seniors and SMBs.
- School and community programs: Expand cyber education in schools through initiatives like the NSW Cyber Security Challenge and support community training delivered via libraries, TAFE, and NFPs, making cyber literacy a lifelong skill.
- Incentives and protections: Introduce tax rebates or vouchers for consumers who purchase certified secure products, and work with insurers to provide premium discounts for households and SMBs that adopt these measures.

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

Industry requires clear, practical guidance on identifying and managing the risks of foreign ownership, control, or influence (FOCI) in technology vendors, as these factors can directly affect supply chain security, data sovereignty, and long-term resilience. Current guidance is fragmented and often focused on critical infrastructure operators, leaving gaps for SMBs, NFPs, and other sectors that rely heavily on overseas technologies.

Key areas where guidance and support are needed:

- Assessment of FOCI risks
    - Government should publish a framework for evaluating vendor FOCI risks, covering ownership structures, board influence, supply chain dependencies, and links to foreign governments
    - This framework could build on existing SOCI Act risk management program requirements but be adapted for broader use, including by SMBs and non-regulated entities.
- Standardised certification and labelling guidance
    - A national certification and labelling framework should make clear which technologies and vendors meet minimum security and sovereignty requirements
    - International examples include Singapore's Cybersecurity Labelling Scheme, the US Cyber Trust Mark, and the UK's PSTI Act. Guidance should also clarify how foreign control of a vendor factors into certification.

- Consistent consumer messaging
    - Government should provide plain-English guidelines to help consumers and businesses understand FOCI risks, clearly showing when a product is locally assured or when it may be influenced by foreign ownership or control
    - Example: Similar to the Australian Energy Regulator's Better Bills Guideline, which standardises consumer information to improve understanding.
- Role of industry bodies in outreach
    - Peak bodies (e.g., COSBOA, AIIA, Australian Banking Association) could help translate government guidance on FOCI into tailored sector resources such as small business cyber health checks or device labelling guides
    - Government support (grants, toolkits, campaign funding) would enable this outreach at scale.
- Incentives and market signals
    - Policy levers are needed to encourage organisations to prefer vendors with transparent ownership and low FOCI risk. Incentives could include procurement preferences, tax rebates, vouchers, or lower insurance premiums for using certified technologies
    - Industry could convene insurers, banks, and vendors into collaborative frameworks, building on existing models like SMB1001 and CyberCert.
- Education and skills development
    - FOCI awareness should be embedded into cyber literacy programs in schools, TAFE, and universities, ensuring the future workforce understands the link between foreign influence and national resilience
    - Industry associations could extend this into professional development and executive training, helping boards and business leaders make more informed vendor choices.

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?

Government has a central role in setting the guardrails for trustworthy data sharing while ensuring industry has clear guidance on compliance and secure practices. The Consumer Data Right (CDR) is a strong Australian example of how consent-driven, standardised frameworks can operate in the banking and energy sectors, and this governance model could be extended into other sensitive domains such as healthcare, telecommunications, and superannuation.

Internationally, there are proven approaches that Australia could adapt:

- The EU GDPR's data portability provisions require clear consent and auditability of data transfers, creating transparency around cross-border flows
- Singapore's Data Protection Trustmark provides a certification scheme that demonstrates an organisation's data protection practices meet rigorous standards — signalling to both consumers and partners that data is handled securely
- The US NIST Privacy Framework offers a voluntary but practical way for organisations to map, assess, and improve data handling practices.

Government could strengthen collaboration with industry by:

- Establishing a national data flow observatory that collects anonymised, sector-wide telemetry on cross-border transfers, with strong privacy protections
- Using existing regulatory touchpoints (ASIC, ACNC, ATO) to require lightweight, standardised reporting of data access and transfer practices, ensuring consistent visibility across sectors
- Supporting industry associations such as the Australian Banking Association, Energy Networks Australia, and Digital Health CRC to act as intermediaries, sharing aggregated insights without exposing sensitive commercial information
- Providing co-funded pilots and data trusts (e.g., similar to UK's Open Banking Implementation Entity) to test secure data-sharing models in critical industries like health, energy, and research.

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?

Government and industry must work together to strike a balance between enabling innovation through data sharing and protecting against IP theft, insider threats and malicious exploitation. This requires both policy leadership from government and practical implementation from industry.

- Government's role: Provide clear regulatory guardrails on secure data sharing (similar to the EU Data Governance Act) and establish safe harbour protections for organisations that meet baseline security and reporting requirements. Co-invest in secure data-sharing infrastructure, such as confidential computing environments and national-scale data trusts. Guidance should also place strong emphasis on managing trusted insider risk, ensuring that access controls, background vetting, and monitoring are part of national data security standards
- Industry's role: Adopt Privacy Enhancing Technologies (PETs), such as tokenisation, encryption, and secure enclaves, to enable safe collaboration while protecting sensitive IP. Collaborate with regulators to design sector-specific playbooks for secure data exchange (e.g., for health, energy, critical minerals). It will also be important that organisations strengthen insider risk management programs, ensuring that staff with access to sensitive data are properly vetted, monitored, and trained, since even strong technical controls can be undermined by misplaced trust.
- Global examples:
    - The UK "Secure Connected Places" program helps local councils adopt IoT securely while enabling Smart Cities innovation
    - Israel's CyberSpark innovation hub co-locates government, academia, and private sector to share data and accelerate secure R&D
    - Germany's Gaia-X initiative creates a federated, secure-by-design data infrastructure for trusted sharing across industries.

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

Guidance should be sector-specific, practical, and internationally aligned, giving organisations a clear path to adopt new technologies securely while maintaining consumer trust.

- Baseline guidance: Provide sector-specific baselines that combine Zero Trust principles, secure software development standards (NIST SSDF, SBOMs), and post-quantum cryptography roadmaps
- AI-specific guidance: Adopt and adapt frameworks like the US NIST AI Risk Management Framework and the EU AI Act to Australian contexts. For example, guidance should cover model provenance, bias testing, adversarial resilience, and responsible deployment in sensitive sectors like healthcare and education
- Cloud and critical systems: Follow the EU Cybersecurity Certification Scheme for Cloud Services (EUCS) by setting tiered assurance levels that make it easier for SMBs and NFPs to select secure cloud providers
- Operational Technology (OT) and Energy Sector: Extend the Australian Energy Sector Cyber Security Framework (AESCSF) to cover new Consumer Energy Resources (CER) technologies (e.g., rooftop solar, EV chargers, smart inverters), aligning with IEC 62443 and IEC 62351.
- Global examples:
    - The Singapore Model AI Governance Framework provides practical, business-friendly guidance for responsible AI adoption
    - The UK National Cyber Security Centre (NCSC) Cloud Security Principles are a model for clear, actionable cloud security guidance
    - The US NIST Cybersecurity Framework 2.0 is embedding emerging tech use cases, providing a flexible standard for new technology adoption.

3.3 Shield 3: World-class threat sharing and blocking

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?

A proactive cyber security posture means shifting industry away from reactive compliance response to anticipatory defence and resilience. Government can enable this by:

- Setting clear cyber security baselines and standards: Regularly update national baselines (e.g., Essential 8 maturity targets) and align them with international standards like NIST CSF 2.0, ISO27001:2022, etc.
- Providing incentives when compliant with standards: Link compliance to insurance premium reductions, procurement eligibility, and tax offsets, rewarding proactive investment in controls
- Fostering sector-wide cyber security exercises: Run cross-sector cyber drills (e.g., energy, finance, health) to encourage preparedness, not just response
- Embedding security in supply chains: Require secure-by-design software and vendor assurance for all government contracts.
- Global example:
    - The US Cybersecurity Maturity Model Certification (CMMC) forces suppliers to demonstrate proactive maturity before bidding on defence contracts (similar to IRAP). Australia could mirror this in critical infrastructure.

25. Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry?

Yes. While Essential 8 provides a strong baseline, government still needs to define what a proactive posture looks like in practice across different industry contexts. Too often, organisations treat Essential 8 (E8) as a compliance checklist rather than a maturity pathway, and many smaller entities struggle to operationalise it without sector-specific guidance.

E8 on its own is not enough. It covers a limited set of controls—mainly focused on Microsoft-based technologies—and does not address the full cyber lifecycle. For example, E8 is largely silent on user awareness and education, which most experts consider one of the highest-value investments today. A national posture must therefore position E8 as a starting point within a broader framework (e.g., NIST CSF, ISO 27001, AESCSF) that addresses governance, resilience, culture, and continuous improvement.

A clearly scoped national posture should:

- Contextualise E8: Provide sector-based roadmaps (e.g. for health, energy, finance, education, SMBs, and NFPs) that show how Essential 8 maturity can be achieved progressively, while also integrating with broader lifecycle frameworks
- Expand beyond prevention: Emphasise resilience measures such as incident response, recovery planning, and supply chain assurance, which are underrepresented by E8
- Update regularly: Refresh guidance as threats evolve, incorporating controls for AI misuse, OT/ICS, and cloud security
- Set clear expectations: Define minimum proactive measures (MFA, backups, patching, monitoring, vulnerability disclosure, and user education programs) that all organisations, regardless of size, should adopt.
- Global example:
    - Singapore's Cybersecurity Code of Practice sets out sector-specific obligations beyond baseline controls, ensuring regulated industries move toward resilience, not just technical compliance.

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

Government can help industry block threats at scale by leveraging mandatory reporting mechanisms, strengthening national threat intelligence platforms, and coordinating action across sectors. Australia already has strong foundations through CIMA (Critical Infrastructure Mandatory Reporting obligations under the SOCI Act) and the CTIS (Cyber Threat Intelligence Sharing) platform, but these need to be expanded and operationalised to achieve true ecosystem-wide blocking.

Key opportunities include:

- Operationalising CIMA data for defence: Reports submitted under CIMA should feed into national threat feeds, ensuring that intelligence from incidents in one sector can be used to protect others. For example, a ransomware IOC reported by an energy operator could be quickly distributed to financial services, telcos, and education providers
- Expanding CTIS into a centralised clearinghouse: Scale up CTIS into a trusted, real-time threat exchange where verified indicators (malicious IPs, phishing domains, malware hashes, scam URLs) can be automatically consumed by ISPs, MSSPs, and critical infrastructure. This could mirror the UK's Active Cyber Defence program, which blocks millions of phishing attempts annually using shared intelligence

- Mandated baseline blocking at network level: Extend telco-led blocking of scam SMS to phishing websites, spoofed domains, and malware command-and-control servers, backed by intelligence sourced from CTIS and CIMA
- Support for low-maturity sectors: Provide access to CTIS feeds and managed security services for sectors such as aged care, education, and local government, which often lack the capacity to implement intelligence-led blocking
- International disruption campaigns: Use CTIS as the backbone for joint operations with Five Eyes, Europol, and ASEAN partners, enabling Australia to participate in coordinated takedowns of malicious infrastructure.
- Global examples:
    - The US CISA Shields Up initiative distributes machine-readable indicators to industry for automated blocking
    - The EU's MeliCERTes threat intelligence platform acts as a central clearinghouse for CERTs across Europe — CTIS could evolve to play the same role in Australia and the Indo-Pacific.

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

Safe browsing technologies are already highly effective but underutilised. Government can amplify their use by:

- Partnering with browser vendors (Google, Microsoft, Mozilla, Apple) to make warning pages clear, accessible, and actionable for non-technical users
- Running awareness campaigns that teach users why warnings appear and how ignoring them increases risk
- Exploring AI-driven detection: Invest in AI that analyses websites in real-time as they load, flagging subtle malicious behaviours invisible to static scanners
- Sector-specific pilots: Test enhanced browser protections in education and healthcare environments, where phishing remains a top threat
- Example: Google's Safe Browsing API already blocks billions of phishing attempts daily. With government support, this capability could be extended into Australian SMB and NFP environments.

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?

A thriving threat-sharing ecosystem requires more than just technology; it needs legal certainty, cultural trust, and incentives for broad participation. While mature sectors such as finance and energy already benefit from established ISACs, many low-maturity sectors — such as aged care, education, local government, and agriculture — lack the resources to set up or engage in structured sharing.

Key enablers include:

- Legal certainty and safe harbour protections: Organisations are often reluctant to share threat data due to concerns about liability, privacy, or regulatory consequences. A government-backed safe harbour framework, similar to the US Cybersecurity Information Sharing Act (CISA) 2015, would give businesses confidence to share intelligence without fear of penalty

- Neutral, trusted exchange platforms: Build on the CTIS (Cyber Threat Intelligence Sharing) platform as a neutral hub for sharing, where organisations of all sizes can both contribute and consume actionable threat intelligence. A neutral backbone helps remove commercial competition as a barrier to collaboration
- Integration of mandatory reporting (CIMA): Leverage Critical Infrastructure Mandatory Reporting obligations (CIMA) to feed anonymised incident and IOC data into CTIS, making this intelligence immediately actionable for other sectors. This would ensure lessons from one industry benefit the entire ecosystem
- Incentives for participation: Offer reduced regulatory reporting requirements or cyber insurance discounts for businesses that actively contribute threat data. For SMBs and NFPs, provide subsidised access to CTIS feeds via MSSPs or sector-based hubs
- Sector-specific ISACs for low-maturity industries: Establish ISACs in sectors such as aged care, education, and local councils, where cyber maturity is low but the risk to communities is high. Seed funding and government facilitation would help overcome resource and trust barriers.
- Global examples:
    - The UK's CiSP platform (Cyber Security Information Sharing Partnership) demonstrates how a government-hosted neutral platform can bring together industry and government in real-time
    - In the US, the FS-ISAC (Financial Services ISAC) and MS-ISAC (Multi-State ISAC for local government) show how both high-maturity and low-maturity sectors benefit from structured sharing.

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

Alignment requires breaking down silos and extending existing threat-sharing models:

- Expand current telco–bank collaboration on scam blocking to include social media platforms, e-commerce marketplaces, and logistics providers
- Create a national threat exchange API where verified IOCs, scam phone numbers, and malicious URLs can be ingested by all sectors in real-time
- Embed scam intelligence into consumer apps: Flag suspicious activity directly in banking apps, government portals, or browser warnings
- International sharing: Link with EU and UK anti-fraud taskforces to share scam typologies that often cross borders.
- Global example:
    - The UK's JMLIT (Joint Money Laundering Intelligence Taskforce) shows how intelligence sharing between banks and government agencies can disrupt financial crime at scale.

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?

Roles and responsibilities between government and industry in a conflict or crisis scenario remain unclear for many sectors, particularly outside of critical infrastructure. While the ACSC provides resources and templates to help organisations create their own incident response playbooks, there is

no single, nationally coordinated framework that defines how these organisational playbooks connect into a whole-of-nation cyber crisis response.

To improve preparedness, government could:

- Publish a National Cyber Crisis Playbook that clearly outlines the respective roles of the ACSC, Home Affairs, Defence, regulators, and industry partners during a large-scale incident. This should align with the ACSC's organisational playbook guidance so businesses can plug their plans into the national framework
- Expand cyber exercises by running multi-sector crisis simulations, similar to NATO's Locked Shields exercise, which test how industry and government coordinate under stress. Exercises should include not just Tier 1 critical infrastructure but also SMBs and NFPs in the supply chain
- Clarify escalation pathways by defining who leads in different scenarios (e.g., ACSC vs. Defence vs. regulators) and how information flows between government and industry during an incident
- Build trust and speed by pre-establishing secure communications channels between government and industry for use in crises.
- Global example:
    - Israel's national cyber crisis exercises bring together government, finance, energy, and health to practise coordinated response, while the US CISA's National Cyber Incident Response Plan (NCIRP) provides a clear national playbook that maps organisational plans into a federal response.

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

Adopting a Vulnerability Disclosure Policy (VDP) helps businesses identify and fix weaknesses before adversaries exploit them, but many organisations are hesitant due to perceived legal, financial, and reputational risks. To encourage adoption, government could create clear incentives, protections, and recognition pathways.

Key government actions:

- Procurement leverage: Require suppliers to government (and eventually critical infrastructure providers) to have a VDP in place, similar to how Essential 8 maturity targets are being embedded into procurement
- Financial incentives: Offer tax offsets, innovation grants, or reduced cyber insurance premiums for companies that publish and maintain a VDP. This would help smaller entities overcome upfront costs
- Legal safe harbour: Introduce protections for companies that accept vulnerability reports in good faith, ensuring they are not penalised for disclosing or remediating reported weaknesses
- Recognition and trust-building: Create a government-backed VDP certification badge that organisations can display publicly (similar to ISO/IEC 27001 or Cyber Essentials certifications), signalling to customers and partners that they take security seriously
- Awareness campaigns: Provide practical toolkits and ACSC-endorsed templates so businesses — particularly SMBs and NFPs — can implement a VDP without needing deep technical or legal resources.

- Global examples:
    - The US DHS Binding Operational Directive 20-01 mandated all federal agencies to adopt VDPs, accelerating private sector adoption
    - The EU Coordinated Vulnerability Disclosure framework provides standardised templates for both government and businesses
    - Japan's Bug Bounty programs via JPCERT/CC show how government can help normalise vulnerability reporting across industries.

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

Yes. A national vulnerability disclosure program (NVDP) is essential to create a safe, consistent, and legally protected pathway for security researchers to report vulnerabilities affecting both public and private sector organisations. Without such a program, many vulnerabilities will remain unreported or are disclosed publicly in unsafe ways.

Why it is needed:

- Safe reporting mechanism: Researchers currently risk legal action under cybercrime or privacy laws if they report vulnerabilities without prior agreement. An NVDP would provide legal protection and safe harbour
- Accelerated patching: Centralising reports reduces duplication and ensures vulnerabilities are triaged and addressed more quickly
- Sector-wide resilience: Vulnerability reports for one organisation (e.g., a cloud service provider) often have downstream impacts across entire supply chains; an NVDP ensures this intelligence is shared
- Support for SMBs and NFPs: Smaller entities often lack dedicated security teams. A national program could provide a government-backed channel to triage reports on their behalf.

How it could work:

- Hosted by ACSC: The program could be run through the ACSC, acting as the trusted broker between researchers and organisations
- Standardised framework: Use clear guidelines based on ISO/IEC 29147 (Vulnerability Disclosure) and ISO/IEC 30111 (Vulnerability Handling Processes)
- Tiered participation: Critical infrastructure operators could be mandated to participate, while SMBs/NFPs could opt-in voluntarily
- Integration with CTIS: Reports from the NVDP could feed into the Cyber Threat Intelligence Sharing (CTIS) platform, ensuring insights are shared across industries once mitigations are available.
- Global examples:
    - The US CISA VDP Platform has enabled thousands of vulnerabilities across federal agencies to be reported and fixed
    - The UK NCSC Vulnerability Reporting Service offers a safe channel for researchers to report issues affecting UK organisations, including private sector entities

- The Dutch NCSC Coordinated Vulnerability Disclosure model is widely seen as a global best practice for balancing researcher, vendor, and government responsibilities.

3.4 Shield 4: Protected critical infrastructure

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

SOCI has been effective in raising awareness of the threats and the need to progressively improve risk management practices. The extent to which SOCI has delivered tangible uplift has been variable across organisations. In general, where organisations have adopted a compliance driven approach, they have realised fewer benefits than those who have recognised that this is an opportunity to drive uplift and improvement in risk management. The level of resources/budget committed to achieving compliance has varied wildly between organisations, even amongst those regarded as peers. We have observed a direct correlation between resources allocated and the benefits realised.

It is hard for a single set of obligations to be truly "proportionate" across such a wide array of organisations ranging from start-ups to major corporations. This inevitably means that the burden is seen as "heavy" by smaller businesses. In our experience, continuing to apply the same level of maturity for all businesses regardless of size/complexity may be problematic and further tailoring should be considered.

In relation to energy generation, the threshold for scoping is not tied to capacity alone but is instead determined by whether an asset is considered critical to the security and reliability of electricity systems. With hindsight, this approach has created challenges for some organisations that would not previously have considered certain assets in their portfolio as "critical." The role of the Cyber and Infrastructure Security Centre (CISC) in setting and communicating the Rules is therefore fundamental, as it provides the practical interpretation of the Act. While this has improved consistency in many cases, the case-by-case nature of criticality determinations has at times led to uncertainty and debate around proportionality.

We have found that the high level of communication from CISC has meant that the rules are generally well understood. However, the areas that have caused confusion in our experience are as follows:

- How the obligation under "cyber and information security hazards" 8(2) which requires cyber risks to be managed co-exists with the obligation in 8(4) to comply with a cyber framework. We have observed confusion as to whether achieving compliance with 8(4) achieves 8(2)
- How to manage the risks relating to workers who may be employed by supply chain partners but meet the definition of "critical worker" for the purposes of the personnel hazard
- How the CIRMP obligations function in a situation where there is a transfer of an asset. If an asset is transferred out of an existing CIRMP to new owners, there is no grace period defined in the act for the new owners to achieve compliance. This has been problematic when one asset is divested from a portfolio of assets that rely on a corporate SOCI program - an asset may be non-compliant on day 1 of the new ownership. Defining a grace period for asset transfer would be helpful
- The requirements relating to "critical workers," as defined in the Act are, in our experience, generally well understood. However, we have noted that the SOCI act does not prescribe organisations to consider "key person" reliance. This is a major risk in some sectors where the challenges of ageing workforce and aged assets are well known. Adding a requirement to para

9(1) of the rules to require consideration of key person reliance would result in a more holistic consideration of personnel risks.

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

The existing cyber obligations provide a broad platform for organisations to take a holistic approach to cyber risk management. However, the current requirement to adopt only one of the named frameworks can lead to very different outcomes when it comes to cyber security. Those organisations who adopted Essential 8 have been able to take a much narrower approach than those who adopt one of the broader standards. Making Essential 8 a mandatory baseline requirement to be supplemented with one of the other frameworks would provide better cyber risk management outcomes.

Over time, prescribing differing levels of maturity based on the size, complexity and perceived criticality of the asset would drive a more proportionate approach.

As Australia begins to better understand the cyber threat posed by AI and the cyber threat to AI implementations in our critical infrastructure assets, further guidance on how to practically assess and mitigate the risks will be essential to ensure that cyber programs keep pace.

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

Covered by the commentary in question 33.

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?

There are number of major service providers who supply critical goods and services to many entities in certain critical infrastructure sectors (e.g., operations and maintenance providers). Whilst they do not fall within any of the prescribed asset classes, they are a key part of Australia's critical infrastructure ecosystem. Each of these suppliers would have been considered and assessed as part of "supply chain" risk by many different industry participants. Across a particular sector, this is a significant duplication of effort. Identifying those suppliers where there is concentration risk and adding them to the asset classes covered by SOCI so that they have to adopt a CIRMP which can then be relied upon by trading partners would reduce effort across the economy and drive a more consistent outcome. It would also contribute towards the notion of critical infrastructure being a system of trusted systems.

Further engagement and guidance on physical security would be helpful. Of the hazard vectors under SOCI, this is where we have observed the greatest tendency to accept the 'status quo' and document existing practice as opposed to thoroughly reviewing whether existing arrangements are appropriate to the risks faced.

In heavily regulated sectors such as power and water, visible and continued engagement between the government and the relevant regulatory bodies is critical to ensure that the Regulatory Reset process and SOCI agendas remain aligned. This would assist in ensuring that industry participants are able to allocate capital to those areas which require uplift to mitigate critical risks.

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

Practical guidance on how to apply Essential 8 to a highly complex business which is comprised of many different assets and technologies would be helpful. This interpretation has been quite challenging for some businesses who have only a portion of their assets in scope for SOCI.

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

This is variable and, in many cases, driven by the risk appetite and previous experience of the Board and Executive leadership. Essential 8 is widely understood and, whilst far from ubiquitous, it is increasingly being adopted by Australian corporates. We have also seen a strong correlation between organisations with leaders who were previously exposed to financial services (and CPS 234) and the appetite to implement and report against government frameworks in other industries. This experience suggests that as CPS230 becomes embedded in financial services, there is the opportunity to establish this approach as de-facto good practice for operational risk management in industry.

3.5 Shield 5: Sovereign capabilities

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 has a pivotal role in shaping the development and growth of Australia's cyber workforce. Beyond funding, its role is to act as a strategic planner, enabler, and convener—setting national priorities, aligning education with industry needs, and creating the policy levers and incentives that encourage investment in skills. By working in partnership with industry bodies, educators, and communities, government can ensure a sustainable pipeline of talent that is resilient to technological disruption, inclusive of diverse pathways, and capable of meeting the rising demand for cyber leadership and expertise.

Strategic workforce planning

- Government: Build a clear, long-term view of cyber workforce demand across sectors.
- Initiatives / pilots / policy ideas:
    - National cyber workforce roadmap: Forecast demand in sectors like energy, health, defence, and critical infrastructure; publish annual workforce gap reports.
    - Sector talent councils: Create advisory groups with industry (e.g., AustCyber, AISA, Energy Networks Australia) to provide continuous feedback on skills demand.
    - Cyber workforce observatory: A data-driven program (similar to the National Skills Commission) to track enrolments, career transitions, and workforce attrition.

Education and training incentives

- Government: Make cyber pathways attractive and accessible for students
- Initiatives / pilots / policy ideas:
    - Cyber scholarships and bursaries: Expand programs targeting under-represented groups (women, First Nations, regional students)
    - Cyber in schools: Expand STEM and coding programs with a cyber security focus (e.g., a national rollout of the NSW Cyber Security Challenge)
    - TAFE cyber fast-track: Develop short-cycle cyber qualifications that allow school leavers or career changers to rapidly enter entry-level roles.

Entry-level pathways

- Government: Replace “apprenticeship-style” early career opportunities being displaced by AI
- Initiatives / pilots / policy ideas:
    - National Cyber Apprenticeship Scheme: Co-designed with industry, modeled on trade apprenticeships, where students combine study with paid placements in SOCs, consulting, and government
    - Public Sector Cadetships: Scale initiatives like the Australian Public Service Digital Cadetship with cyber-specific streams
    - AI-Augmented SOC Training Pilot: Partner with vendors (e.g., Microsoft, CrowdStrike) to provide apprenticeships in AI-enabled SOC environments, ensuring graduates learn to work alongside automation.

Mid-career re-skilling

- Government: Broaden the talent pool by bringing in professionals from adjacent sectors
- Initiatives / pilots / policy ideas:
    - Cyber retraining academy: Modelled on the UK Cyber Retraining Academy, offering intensive programs for IT, defence, and engineering workers to transition into cyber
    - Cyber to critical infrastructure pathways: Programs that train electricians, control engineers, and OT operators in IEC 62443 and AESCSF-aligned cyber practices
    - Micro-credentialing framework: Nationally recognised micro-credentials (delivered via TAFE/universities) for areas like cloud security, OT security, and GRC.

Industry partnership and ecosystem building

- Government: Work with industry bodies to amplify training, mentoring, and career development
- Initiatives / pilots / policy ideas:
    - Cyber mentorship exchange: Government-funded mentoring programs run by AISA and AustCyber, pairing students with industry leaders
    - Certification and career pathway standards: Work with COSBOA, AIIA, and industry to establish nationally recognised cyber job families (aligned to frameworks like NICE)
    - SMB & NFP Cyber Workforce Uplift Fund: Grants for small businesses and NFPs to access interns/apprentices, creating training capacity while uplifting cyber maturity.

Regional and community outreach

- Government: Ensure workforce growth is inclusive and not concentrated in major cities
- Initiatives / pilots / policy ideas:
    - Regional cyber hubs: Expand on the Regional Tech Hub model with dedicated cyber training and awareness centres
    - Cyber in community colleges and libraries: Partner with local councils and TAFEs to provide free or low-cost cyber awareness courses

- NFP partnership grants: Fund NFPs to deliver grassroots cyber upskilling programs in vulnerable communities.

International benchmarking and collaboration

- Government: Align Australia's cyber workforce initiatives with global best practice
- Initiatives / pilots / policy ideas:
  - CyberCorps: Scholarship for Service (US Model): Fund students in return for service in government cyber roles
  - Singapore's Cybersecurity Professional Scheme: Create structured job families and career progression frameworks across public and private sector
  - Trans-Tasman Cyber Exchange Program: Exchange placements with NZ cyber agencies and companies to broaden exposure and training.

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?

Australia and international partners have trialled a range of initiatives to make cyber more accessible to mid-career professionals and under-represented groups. The most successful programs are those that combine practical training with structured pathways into employment, supported by mentoring and financial incentives.

- Mid-career transitions: UK Cyber Retraining Academy, US CyberCorps Scholarship-for-Service (public-sector placement), vendor-backed programs like AWS re/Start, Microsoft Career Connector, Australian CSCRC internships and APS Digital/Cyber cadetships—all pair short, job-relevant training with guaranteed placements/mentors
- Diversity: Women in Cyber (AustCyber/AISA), She Codes Australia, Girls in Tech, Return-to-Work tech pathways (micro-credentials + flexible placements), and First Nations digital skills scholarships. The common success factor is paid, structured on-ramps (mentored projects, internships, apprenticeships) rather than training-only.

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?

Cyber security draws on a wide range of technical, risk management, and investigative skill sets that exist across other industries.

- Immediate pathways: IT ops, networking, sysadmin, software engineering, cloud/platform, service desk → SOC analyst, incident responder, cloud security, appsec
- OT/critical infrastructure: Electrical/control engineers, SCADA/field techs (energy, water, rail, mining) → OT/ICS security aligned to IEC 62443/AESCSF
- Risk and assurance: Audit, compliance, safety engineering, procurement/supply chain → GRC, third-party risk, privacy/security-by-design
- Investigation and intel: Law enforcement, defence, fraud analytics → threat intel, DFIR
- Research/data to leverage: (i) ISC² Cybersecurity Workforce Study (skills gaps and role profiles), (ii) NICE/NIST work role framework (task-to-skill mapping), (iii) Lightcast/Burning

Glass market analyses for Australian cyber roles, (iv) AustCyber sector competitiveness reports (training and demand signals).

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?

Solving Australia's cyber challenges requires collaboration across sectors to ensure research is aligned to real-world needs and rapidly translated into practical impact. Coordination between government, academia, think tanks, and industry can sharpen priorities, avoid duplication, and direct resources to the areas of greatest national benefit.

National missions and challenge grants

- Government could define 5–6 "national cyber missions" aligned to Australia's strategic priorities—such as operational technology (OT) and consumer energy resource (CER) security, privacy-preserving analytics for healthcare data, post-quantum readiness, and secure AI adoption in critical sectors. These would be supported through co-funded challenge rounds, where consortia of universities, think tanks, and companies compete to deliver time-boxed demonstrators.
- Global examples:
    - The US DARPA Grand Challenges and the UK Defence and Security Accelerator (DASA) both use mission-driven challenges to accelerate solutions in national security - a similar approach could be tailored for cyber in Australia.

Translational pathways

- Many strong research outcomes in Australia stall due to a "valley of death" between lab and deployment. Expanding ARC Linkage grants and Cooperative Research Centres (CRCs) with faster procurement pathways would enable pilots to move rapidly into government and critical infrastructure environments. Standardising IP-sharing, licensing, and data-use agreements would reduce friction for industry–academic collaboration.
- Example:
    - The Cyber Security CRC has already demonstrated value by embedding researchers with industry partners like the energy sector; this could be scaled with rapid adoption mechanisms modelled on the US In-Q-Tel venture partnership model.

Shared testbeds and **secure data sandboxes**

- Government could fund sector-specific cyber test labs (for energy networks, health systems, and transport) where academia, industry, and think tanks can experiment with de-identified datasets, operational environments, and cyber-physical systems. These testbeds should include privacy-enhancing technologies (PETs) such as trusted execution environments (TEEs), federated learning, and differential privacy, and allow red and blue team testing in controlled conditions.
- Global example:
    - The European Union's European Cybersecurity Competence Centre (ECCC) funds sectoral labs across member states to provide this type of shared facility.

People mobility and capability exchange

- To close the gap between policy, research, and industry, government could fund practitioner-in-residence programs (industry professionals placed in universities), policy fellowships (academics embedded in Home Affairs or Defence), and joint appointments that allow cyber experts to move fluidly between research and operational environments.
- Global examples:
    - The US Presidential Innovation Fellows program and the UK Cabinet Office's Tech Secondments bring private-sector talent directly into government; Australia could mirror these with a cyber-specific focus.

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

Government and academia already collaborate in cyber security, but these partnerships are often limited to short-term funding cycles and siloed projects. To create a more sustainable, trusted research–policy ecosystem, Australia needs mechanisms that embed collaboration into everyday practice, ensure continuity beyond grant programs, and enable knowledge to flow both ways.

Two-way secondments and embedded fellowships

- Establish structured 6–12 month policy or technical fellowships where academics and PhD candidates are embedded in government agencies, and public servants are placed in universities or cyber research centres. This could include placements in ACSC, Defence Science and Technology Group (DSTG), or Home Affairs cyber policy teams. Creating a standing Cyber Policy Lab network, hosted across major universities, would provide a permanent hub where researchers, policymakers, and students co-develop solutions.
- Global example:
    - The UK's Royal Society Pairing Scheme embeds scientists in Parliament, while the US Presidential Innovation Fellows place technologists into federal agencies. A cyber-specific adaptation would bring immediate value in Australia.

Standardised collaboration frameworks

- Develop a collaboration toolkit with model IP clauses, data-use and ethics templates, and a "fast-track" security clearance process for vetted researchers who need access to sensitive datasets. This would remove legal and bureaucratic barriers that often delay or prevent partnerships.
- Example:
    - The ARC Industrial Transformation Research Hubs provide model collaboration agreements—these could be extended with a cyber lens.

Talent pipelines through education partnerships

- Expand co-supervised PhDs and Masters programs, where projects are co-designed by universities and government agencies to solve live policy or technical problems. Introduce cyber micro-credentials co-developed with agencies (e.g., on OT security, AI assurance, or threat intelligence) that can be stacked into formal qualifications. Capstone projects should be aligned with real government problem statements, with an adoption pathway built in.

- Global example:
    - The Cyber Security CRC has pioneered these models, but scaling nationally (like Singapore's Cybersecurity Professional Scheme) would embed cyber talent pipelines more deeply.

Open evaluation and shared resources

- Government and academia should jointly publish benchmark datasets, reference architectures, and repeatable test methods to improve transparency and accelerate innovation. This could include shared OT security testbeds, AI model assurance benchmarks, or privacy-enhancing technology sandboxes.
- Global example:
    - The European Cybersecurity Competence Centre (ECCC) coordinates shared datasets and labs across member states; Australia could replicate this approach with a national set of open evaluation resources.

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

Building sovereign cyber capabilities requires a structured, transparent, and criteria-driven method for prioritisation. Australia should focus not only on technologies that reduce foreign dependence, but also on those that underpin critical infrastructure resilience and offer export potential to build long-term competitiveness.

Decision framework

Candidate capabilities should be assessed against clear criteria:

- National security criticality – e.g., whether the capability protects critical infrastructure sectors such as energy, defence, and health
- Economic leverage – ability to reduce costs, create jobs, or strengthen high-value industries such as defence and advanced manufacturing
- Concentration risk – reducing dependence on a small number of foreign suppliers in areas like cloud, semiconductors, or OT tooling
- Feasibility and time-to-build – prioritising areas where Australia has existing research strengths or market footholds
- Export potential – alignment with regional markets, enabling Australian firms to scale globally
- Example:
    - The Critical Technologies in the National Interest list provides a starting point for applying these criteria.

Priority domains

- OT/ICS security tooling and services: Strengthen sovereign providers supporting energy, mining, water, and transport operators, aligned with AESCSF and IEC 62443
- Post-quantum cryptography (PQC) and key management: Build on Australian research expertise to develop sovereign PKI and key escrow solutions, ensuring resilience in finance and defence
- Identity and trust services: Expand local innovation in digital ID and authentication solutions (e.g., myGovID, ConnectID) to reduce reliance on foreign identity providers

- Secure silicon and firmware assurance: Invest in hardware trust anchors and supply chain verification to address concentration risks in semiconductors, networking equipment, and IoT
- Threat intelligence & DFIR: Strengthen sovereign cyber intelligence capabilities, with Australian firms providing regional threat intelligence sharing and incident response capacity
- Secure-by-design software pipelines: Incentivise adoption of SBOMs (Software Bill of Materials) and NIST SSDF-aligned secure development lifecycles, creating sovereign software assurance industries.
- Global example:
    - Israel's investment in cyber range training platforms shows how niche sovereign tools can become global exports.

Policy levers

- Anchor-tenant procurement: Government commits to buying from sovereign vendors in areas such as OT monitoring, PQC, or DFIR, creating guaranteed early demand
- Mission-linked grants and tax credits: Similar to the US CHIPS Act or Singapore's Cybersecurity Industry Call for Innovation, tie funding to specific sovereign capability missions
- Standards conformance as a market access requirement: Mandate that vendors in sensitive domains (e.g., CER, OT) meet AESCSF or IEC 62443 standards, giving sovereign providers a competitive edge
- Cluster development: Create sovereign capability clusters linking universities, startups, and testbeds (e.g., an OT Security Hub co-located with energy utilities, or a PQC hub around leading universities).
- Global example:
    - The UK's National Cyber Security Centre (NCSC) Industry 100 program and Singapore's Cybersecurity Industry Call for Innovation both show how procurement and clustering can accelerate capability building.

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 faces significant risks from over-reliance on a small number of global technology providers, critical infrastructure chokepoints, and fragile supply chains. ICT concentration creates systemic vulnerabilities where a single point of failure, outage, or geopolitical disruption could have widespread national consequences. Addressing these risks requires forward-looking policies that diversify providers, build redundancy, and invest in sovereign or regional alternatives.

Concentration risks

- Cloud and SaaS dependence:
    - Australia relies heavily on three global hyperscalers (AWS, Microsoft Azure, Google Cloud) for hosting, identity services, and productivity software. A major outage, misconfiguration, or sanctions event could disrupt government services, finance, or healthcare.
    - Example:
        - The 2023 Microsoft 365 global outage disrupted email and Teams for banks, hospitals, and universities worldwide.

- Critical comms and cables:
    - Australia has only a limited number of submarine cable routes for international connectivity, and a handful of internet exchange points (IXPs). Damage, sabotage, or geopolitical conflict could sever critical data flows.
    - Global example:
        - The 2022 Tonga cable break left the country offline for weeks, demonstrating fragility in undersea connectivity.
- Software monocultures:
    - Many agencies and businesses run single-vendor stacks for productivity suites, email, or OT/SCADA systems, creating systemic risks if vulnerabilities are discovered.
    - Example:
        - The 2021 Microsoft Exchange vulnerabilities had cascading effects across government and business worldwide.
- Hardware and semiconductor fragility:
    - Australia depends on offshore supply chains for routers, switches, firewalls, and OT controllers. Concentration in East Asian manufacturing (Taiwan, South Korea, China) creates risk exposure to natural disasters and geopolitical tensions.

Mitigation strategies

- Portability and exit planning:
    - Mandate data portability, open APIs, SBOMs (Software Bill of Materials), and log egress to reduce vendor lock-in
    - Require agencies to test multi-cloud or cloud-exit runbooks annually to prove portability.
    - Global example:
        - The UK G-Cloud procurement framework enforces portability requirements for all approved suppliers.
- Diverse routes and resilience in communications:
    - Co-invest in additional submarine cables and domestic IXPs, ensuring geographic diversity of landing points
    - Fund domestic caching, backhaul redundancy, and sovereign satellite internet options to improve resilience.
    - Global example:
        - The Coral Sea Cable System (Australia–PNG–Solomon Islands) improved redundancy for Pacific partners; similar investment is needed for Australia's domestic resilience.
- Assurance and segmentation in OT/critical apps:
    - Require network segmentation, least-privilege access, and backup control paths for critical systems
    - Avoid over-reliance on single identity providers (e.g., enforce federated identity across multiple vendors).

- Global example:
  - The US Colonial Pipeline incident (2021) showed how a single compromised VPN account halted critical fuel supply. Segmentation and alternative control paths would have limited the impact.

- Market development and sovereign capability:
  - Support the growth of sovereign or regional cloud zones (e.g., the Canberra Data Centres model) to provide alternatives to global hyperscalers
  - Develop a vetted marketplace of MSP/MSSPs to avoid concentration in a few providers servicing critical infrastructure
  - Create strategic reserves for semiconductors and critical networking hardware, similar to how governments stockpile fuel.
  - Global example:
    - The US CHIPS and Science Act (2022) invest in domestic semiconductor manufacturing to reduce reliance on foreign supply chains.

3.6 Shield 6: Strong region and global leadership

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?

Attribution, advisories, and sanctions can be effective tools to deter state-sponsored threats and signal Australia's position on malicious cyber activity. However, attribution is technically complex, politically sensitive, and increasingly difficult to prove given the rise of "as-a-service" criminal groups that share infrastructure and tradecraft. While naming threat actors can raise awareness, accuracy and credibility are essential to avoid unintended consequences.

These tools should therefore be complemented by broader strategies focused on education, resilience, and proactive defence, ensuring organisations and citizens understand threats and adopt best practices to reduce exposure.

Considerations

- Develop a transparent national framework for attribution, similar to the UK NCSC's public attribution protocols, to ensure consistency and credibility
- Coordinate with allies (Five Eyes, QUAD, ASEAN partners) for joint advisories and sanctions, following the model of the EU Cyber Diplomacy Toolbox, which enables collective sanctions against cyber aggressors
- Target the enablers of cybercrime (e.g., hosting providers, cryptocurrency mixers, infrastructure operators) as the US has done under its OFAC cyber sanctions regime
- Expand regional information-sharing, mirroring NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) which brings together government, academia, and industry for regional collaboration.

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 has already invested in regional capacity-building through programs such as Cyber RAPID and SEA-PAC Cyber, but deeper partnerships are needed to strengthen collective resilience. Engagement should extend beyond funding to include long-term institutional partnerships, shared exercises, and the promotion of regional norms.

Considerations

- Expand joint CERT development, training, and exchanges, similar to the Asia-Pacific CERT (APCERT) model, which has successfully enhanced incident response across the region
- Support regional cyber drills and simulations, aligned with the EU's Cyber Europe exercise model, to strengthen collective crisis response
- Promote cyber norms through ASEAN and Pacific Islands Forum, drawing from the UN Group of Governmental Experts (UN GGE) frameworks on responsible state behaviour in cyberspace
- Provide sector-specific assistance (e.g., in energy, healthcare, and finance), following the approach of Japan's JPCERT/CC, which provides technical aid to regional partners.

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

Cyber RAPID could evolve from a primarily reactive program into a comprehensive resilience-building platform that strengthens regional capacity before, during, and after incidents. This includes proactive risk assessments, executive-level training, workforce development, and stronger information-sharing arrangements. Addressing the cyber talent shortage in the region will be critical, requiring closer partnerships with academia, industry, and community organisations.

Considerations

- Extend RAPID to include proactive threat hunting and intelligence sharing, similar to the EU's Cyber Rapid Response Teams (CRRTs) which deploy teams of experts across borders
- Integrate RAPID into regional disaster recovery and resilience planning, as done under ASEAN's Disaster Management frameworks, where cyber resilience could be embedded
- Use RAPID as a platform for joint cyber simulations and tabletop exercises, modeled on NATO's Locked Shields exercise, which has become the world's largest cyber defence drill
- Partner with local universities and vocational institutions to build a regional cyber talent pipeline, following Singapore's Cybersecurity Career Mentorship Program that connects students to practitioners
- Establish secondment and knowledge-sharing programs, similar to the EU's Erasmus+ mobility scheme, to strengthen regional exchanges of skills and experience
- Provide community-level awareness and hygiene training in underserved areas, drawing lessons from the US Cybersecurity Awareness Month campaign, which has been adapted internationally.

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?

Australia has an opportunity to play a leadership role in shaping global and regional cyber norms by prioritising engagement in forums where its voice can have the greatest influence. Given Australia's position as a trusted democracy and regional power, it can act as a bridge between global standard-setting bodies and the Indo-Pacific region, ensuring regional concerns are reflected in international frameworks.

Key forums to prioritise:

- UN Open-Ended Working Group (UN OEWG): Influence global discussions on responsible state behaviour in cyberspace, particularly in protecting critical infrastructure
- ASEAN and APEC: Use Australia's strong ties to shape regional cyber resilience standards, building trust with Southeast Asia and Pacific partners
- Global Forum on Cyber Expertise (GFCE): Contribute practical expertise in capacity building and cyber hygiene, especially in the Pacific
- Internet Governance Forum (IGF): Position Australia as a defender of human rights and inclusive internet governance.

Priority issues where Australia can lead

- Norms for responsible state behaviour: Advocate for adoption of UN cyber norms in the Indo-Pacific, promoting restraint from targeting critical infrastructure
- Secure-by-design technology standards: Lead efforts in ASEAN/APEC to embed AI and IoT security into digital trade standards
- Data sovereignty and secure flows: Promote models that balance sovereignty, security, and privacy, drawing on GDPR (EU) and Data Protection Trustmark (Singapore).

Considerations

- Lead regional working groups on AI and IoT security in APEC/ASEAN
- Champion privacy and human rights in cyber governance at the IGF
- Push for harmonised digital trade standards that integrate cyber security, enabling SMEs to participate securely in the global economy.

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

Fragmented international regulatory requirements create a complex environment for Australian businesses. Australia should seek to align with global standards where practical, while positioning itself as a regional leader that supports SMEs and critical infrastructure operators in meeting these requirements.

Priority areas for alignment

- ISO and NIST standards: Ensure Australian frameworks (e.g., AESCSF, Essential 8) map cleanly to global baselines such as ISO/IEC 27001 and NIST CSF 2.0
- EU frameworks (GDPR, NIS2, Cyber Resilience Act): Monitor and adapt compatible principles for privacy and critical infrastructure resilience, ensuring Australian organisations can trade and interoperate securely with EU markets

- Mutual recognition of certifications: Pursue agreements that recognise equivalence between CyberCert/SMB1001 and frameworks such as Cyber Essentials (UK) or Singapore's Cybersecurity Labelling Scheme.

Suggestions for action

- Develop bilateral agreements with partners like the US, EU, Japan, and Singapore for vendor vetting, secure data sharing, and supply chain security
- Create a national "cyber compliance hub" to help Australian businesses navigate overlapping obligations
- Set a baseline of recommended controls (Essential 8 + AESCSF core) and promote them internationally as an interoperable minimum
- Use digital trade agreements (e.g., the Digital Economy Partnership Agreement between Singapore, Chile, and NZ) as vehicles to embed consistent cyber and privacy protections.