Charting New Horizons

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

Name : [redacted]

Tel: [redacted]

Responded Questions	Not Responded
1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 13, 14, 16, 18, 21, 24, 30, 33, 34, 35, 36, 39, 41, 42, 50	5, 12, 15, 17, 19, 20, 22, 23, 25, 26, 27, 28, 29, 31, 32, 37, 38, 40, 43, 44, 45, 46, 47, 48, 49

General Strategic Questions

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?

The rise of AI and machine learning is enhancing advanced defense capabilities, such as predictive threat detection. At the same time, it gives adversaries tools such as AI-driven phishing and automated vulnerability exploits, as seen in recent deepfake scams and adaptive malware attacks.

Quantum computing developments, though still emerging, pose a long-term strategic risk by potentially making current cryptographic methods obsolete, emphasizing the need for early adoption of quantum-resistant encryption standards, as noted in research by NIST and the Australian Signals Directorate.

The growth of IoT and edge devices, projected to exceed 32 connected devices per household in Australia by 2027, will significantly increase the attack surface, especially across critical infrastructure, industrial systems, and smart home networks.

The rapid expansion of consumer energy resources (CER), with over four million rooftop solar systems already in place nationwide, introduces cyber vulnerabilities into the energy grid, creating potential entry points for disruption if not secured through strong standards and monitoring frameworks.

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 programs could be expanded nationally to strengthen cyber resilience. Examples include NSW's Cyber Security Innovation Node and Victoria's Cyber Security Skills Framework, which support local innovation and workforce development; Queensland's Small Business Cyber Security Program, providing practical toolkits and subsidized services; and South Australia's Critical Infrastructure Uplift initiatives, which improve sector-specific resilience. Scaling these programs across jurisdictions could deliver consistent capability growth, reduce

duplication, and ensure that both metropolitan and regional communities benefit from proven approaches.

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

Yes, the high-level Model aligns well with a structured, outcome-focused approach to cyber policy. Its clear connection between interventions, desired outcomes, and measurable “North Star” goals offers a solid foundation for accountability. However, improvements could include more explicit integration of adaptive feedback loops to enable quick policy adjustments in response to emerging threats, sector-specific metrics to reflect different maturity levels across industries, and a stronger focus on measuring the preventive impact, not just incident response results, to better assess long-term resilience.

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

A more effective way to monitor cybersecurity outcomes is to prioritize telemetry as the main enabler of continuous insight, incorporating real-time threat intelligence feeds from ISPs, cloud providers, and critical infrastructure operators to identify attack patterns and vulnerabilities quickly. This can be enhanced by expanding existing reporting mechanisms like the ACSC Annual Cyber Threat Report and SOCI Act obligations, conducting regular national cyber resilience surveys for SMEs, NFPs, and households, deploying automated compliance dashboards connected to regulatory portals, running post-incident debrief programs to gather lessons learned, and enabling secure, crowdsourced vulnerability and scam reporting. Together, these steps would create timely, data-driven feedback loops to improve policy decisions and strengthen resilience.

Shield 1 – Strong Businesses and Citizens

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

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?

The government could improve its cyber awareness efforts by creating a nationally branded, community-driven program, such as **“CyberChamps,”** that unifies messaging across all jurisdictions and channels. CyberChamps would train and certify local “cyber ambassadors” from schools, community groups, libraries, small business networks, and vulnerable community advocates. These ambassadors would provide consistent, practical, and culturally appropriate cyber safety advice using government-approved content, ensuring outreach in metropolitan, regional, and remote areas.

This model could build on lessons from successful pilots, such as the Cyber Wardens program for small businesses and the eSafety Commissioner’s school outreach, while

expanding its scope to include peer-to-peer learning, gamified challenges, and local recognition initiatives. By integrating CyberChamps into education and community systems and partnering with both educational institutions (schools, TAFEs, universities) and technical experts (industry, CERTs, security vendors), the program could grow rapidly, foster trust in cyber advice, and establish a visible, personal contact point for cyber resilience across Australia.

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.)?

The government can increase the adoption of existing cyber resources among SMBs and NFPs by making access easier, more visible, and incentivized. A centralized one-stop cyber portal could combine services such as the Small Business Cyber Resilience Service, Cyber Wardens, and ACNC guidance, with customized pathways tailored to different sectors and sizes. Adoption could be further encouraged through incentives and subsidies such as tax offsets, grants, or reduced cyber insurance premiums for organizations that complete accredited training or implement baseline controls. Collaborating with industry peak bodies to incorporate these resources into membership benefits, providing outreach through chambers of commerce and community hubs, and launching targeted “Cyber Health Check” campaigns that offer quick, no-cost assessments would make adoption rewarding and straightforward. By combining easy access, trusted advocacy, and tangible benefits, the government can help make cyber resilience a standard business practice for SMBs and NFPs.

8. How can industry at all levels and government work together to drive the uptake of cyber security actions by SMBs and the NFP sector to enhance our national cyber resilience? What type of support would be useful and who should provide it?

Industry and government can accelerate cybersecurity efforts for SMBs and NFPs by implementing a coordinated partnership model similar to the UK’s Cyber Essentials. In the UK, the government establishes a straightforward baseline for cyber hygiene, industry groups support its adoption through sector networks, and approved assessors provide affordable certification and guidance. This strategy fosters trust, enhances market reputation, and links certification to tangible benefits, such as procurement eligibility and insurance discounts.

In Australia, a similar approach could have the Australian Government establish a nationally recognized SMB/NFP cybersecurity standard, co-developed with industry. Meanwhile, peak organizations, insurers, and large companies would promote and incorporate it into supply chains. Support could include subsidized assessments, free toolkits, and mentorship programs delivered through trusted partners, such as chambers of commerce, professional associations, and community networks. This collaborative strategy would leverage government authority, industry influence, and market incentives to create a scalable framework for nationwide cybersecurity resilience.

9. What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFPs? What role should government play in supporting/endorsing SMB tailored standards?

Several existing and emerging cybersecurity standards could be adapted to enhance the resilience of SMBs and NFPs, drawing on both global best practices and local contexts. Internationally, the UK's Cyber Essentials framework provides a simple, low-cost certification process covering five key technical controls, and has proven effective in increasing baseline security while incentivising adoption through procurement requirements. Similarly, the **US NIST Cybersecurity Framework (CSF)** offers a scalable, risk-based approach that can be simplified for smaller entities. At the same time, **Singapore's Cyber Essentials and Cyber Trust** marks provide tiered recognition to encourage progression from basic to advanced maturity.

In Australia, these models could be adapted into a Cyber Standard that combines international benchmarks with sector-specific guidance, delivered in clear language and supported by practical implementation tools. The government's role should include endorsement, funding, and facilitation to promote the standard, fostering national consistency and trust. This would involve providing financial support for accreditation, training, and toolkits, as well as collaborating with industry bodies to embed the standard into supply chains, insurance assessments, and grant eligibility criteria. Additionally, the government could establish a national cyber mark or certification recognized across industries, supported by ongoing awareness campaigns and linked to clear benefits such as tax offsets, lower insurance premiums, and eligibility for government contracts.

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?

Not-for-profit (NFP) entities face unique cybersecurity challenges compared to the broader business sector, primarily due to limited budgets, restricted IT resources, and a workforce that is often heavily reliant on volunteers. This leads to high turnover, inconsistent cybersecurity awareness, and limited access to specialized skills. Despite these limitations, NFPs frequently manage high-value, sensitive personal and financial data, including donor, beneficiary, and health information, making them appealing targets for malicious actors. Smaller NFPs also tend to lack formal governance frameworks and dedicated cybersecurity policies, relying instead on ad-hoc measures when incidents occur.

Government interventions with the most significant impact should focus on affordable, sector-specific capacity building that tackles both resource and skills gaps. A key step could be to promote, curate, and support the deployment of vetted open-source cybersecurity solutions tailored for NFP settings. Proven tools like pfSense (firewall), Wazuh (SIEM), Cryptomator (file encryption), and KeePassXC (password management) can deliver enterprise-grade security at a minimal cost if implemented appropriately. To maximize adoption, the government could launch a nationally endorsed "Open-Source Cyber Security Toolkit for NFPs," complete with deployment guides, training modules, and a list of trusted providers for optional paid support.

This should be complemented by fully subsidized cyber awareness and incident response training tailored to NFP operations, as well as grants or vouchers for essential security investments (e.g., MFA deployment, secure hosting, endpoint protection). Additionally, inclusion in threat intelligence sharing networks is crucial for receiving timely alerts. Establishing a cyber mentor network pairing smaller NFPs with experienced IT or security professionals would further help bridge the skills gap. By combining free, high-quality open-source solutions with structured guidance, training, and targeted funding, the government can significantly enhance the NFP sector's cyber resilience while conserving scarce resources for mission delivery.

11. Do you consider cyber insurance products to be affordable and accessible, particularly for SMBs? If not, what factors are holding back uptake of cyber insurance?

For many SMBs, cyber insurance products remain neither fully affordable nor easily accessible, with cost, complexity, and eligibility requirements being key barriers. Premiums have risen sharply in recent years, often by 50–100% in some markets, due to the increasing frequency and severity of cyber incidents. Globally, this trend is consistent: in the United States, the National Association of Insurance Commissioners reported double-digit premium increases from 2021 to 2023, while in the UK, the Association of British Insurers noted an average cost increase of over 50% for some SME cyber policies following the 2021 ransomware spikes. In Australia, from industry circles, I understand that premiums are often prohibitively high for smaller entities, and coverage can be difficult to secure without meeting advanced cyber hygiene requirements, such as multifactor authentication, endpoint detection and response, and documented incident response plans.

Accessibility is further hindered by technical underwriting criteria that many SMBs struggle to meet. Insurers in markets like Singapore and Canada have introduced **"minimum controls checklists"** before issuing policies, a practice that, while improving overall security, can exclude less mature organisations. Additionally, a lack of awareness about what cyber insurance covers and confusion between stand-alone and add-on policies reduces uptake.

To improve both affordability and accessibility, international examples such as the UK's Cyber Essentials-linked insurance model could be considered, where meeting a government-endorsed baseline standard provides access to simplified, lower-cost coverage. Similarly, New Zealand's sector-specific group policies for SMEs offer collective bargaining power and reduced premiums. Adopting these models in Australia, potentially with government-backed risk pools or subsidies for high-risk sectors, could help bridge the affordability gap while driving an uplift in baseline cyber maturity.

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

The threat of ransomware is well understood at a conceptual level by many businesses and individuals, namely that it involves malicious actors encrypting data and demanding payment for its release. However, a practical understanding of the evolving tactics remains limited, particularly among small entities. While awareness often centres on phishing as the main entry point, modern ransomware increasingly

leverages supply chain compromises, remote desktop protocol (RDP) exploitation, and multi-extortion tactics (data theft, public shaming, and secondary attacks). Globally, the rise of ransomware-as-a-service (RaaS) and AI-powered social engineering has lowered the barrier to entry for attackers, making attacks faster, more targeted, and more operationally disruptive.

To counter this, government could adopt a multi-layered support model that includes mandatory ransomware incident reporting (as in the US and parts of the EU), national ransomware readiness exercises for SMBs and high-risk sectors (similar to the UK's "Exercise in a Box"), and subsidised access to EDR tools, secure backup solutions, and patch management services for small entities. Public awareness campaigns should evolve to address modern attack vectors beyond phishing and supply practical recovery playbooks.

A core pillar should be a **National No-Pay Policy Framework**, establishing a clear position that discourages or prohibits ransom payments to disrupt criminal business models. This framework would require prompt incident reporting, mandate transparency in ransom-related negotiations, and provide legal safe harbours for compliant victims. To succeed, it must be supported by strong law enforcement and diplomatic coordination through initiatives like the Counter Ransomware Initiative, and backed by rapid response support services that cover incident containment, forensics, and communications, so that paying a ransom is never perceived as the quickest or only recovery option. International experience, such as the Netherlands' no-pay approach, demonstrates that when combined with robust recovery support, this policy can reduce payment rates and disrupt criminal networks.

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 & NFPs. Smaller organisations consistently exhibit low adoption of control measures (MFA, patching, backups) and are disproportionately represented in phishing, credential theft, and ransomware breaches. Global telemetry (DBIR 2025) reveals that social engineering and credential misuse are the primary drivers of SMB incidents, with constrained budgets and limited skills exacerbating the risk.

Healthcare & essential services. Health remains a prime target for ransomware; the consequences extend beyond data loss to delayed care and safety risks. ENISA highlights availability attacks and ransomware among top threats; independent studies and sector reporting continue to link cyber incidents to clinical disruption

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

The most important regulations for reducing overall cyber risk in Australia are those that set clear, enforceable security baselines across critical sectors and high-value data environments. The Security of Critical Infrastructure Act 2018 (SOCI Act) plays a central role by mandating risk management programs and enhanced cyber obligations for systems of national significance. Meanwhile, the Privacy Act 1988, particularly

under Australian Privacy Principle 11, establishes obligations to protect personal information from misuse and unauthorized access. The Australian Prudential Regulation Authority's CPS 234 standard is also vital, ensuring regulated financial institutions maintain proportionate information security capabilities. Additionally, directors' duties under the Corporations Act, when interpreted through the lens of cyber risk, create governance-level accountability for security outcomes.

There are notable regulatory gaps. Australia still lacks a harmonised national cybersecurity standard for SMBs and NFPs, despite these sectors representing a large portion of the economy and a significant supply chain vulnerability. The current patchwork of requirements across industries creates compliance complexity without guaranteeing consistent uplift. Similarly, there is no clear legislative framework for vulnerability disclosure, limiting the safe engagement of security researchers. Finally, while ransomware payment reporting is now in place, there is no unified "no-pay" policy or mandatory baseline controls for all high-risk entities, resulting in uneven preparedness and response capabilities across sectors. Addressing these gaps would strengthen resilience beyond critical infrastructure and large enterprises, making security expectations more transparent and more enforceable across the whole economy.

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?

For OT anchor, both regulation and procurement on ISA/IEC 62443 are required to make security measurable and enforceable across the lifecycle. Use zones-and-conduits for segmentation, require secure-by-design development and patchability from vendors, and mandate supplier assurance (e.g., SBOMs, vulnerability disclosure, support windows) as conditions of purchase and integration. Operationalise this with NIST SP 800-82 Rev.3: complete asset inventories, apply least-privilege network architecture, harden interfaces between IT/OT, establish monitoring with anomaly detection tuned for process environments, and run rehearsed incident response that prioritises safety and availability.

For smaller or resource-constrained operators, adopt CISA's Cross-Sector Cybersecurity Performance Goals as the pragmatic baseline (MFA, backups, logging, EDR where feasible, vulnerability and patch management), then phase up to 62443 conformance over time. Combine this with targeted audits and red-team exercises (safety-aware), and tie compliance to licensing and government procurement. The result is a balanced approach that respects OT safety constraints while delivering clear controls and vendor accountability across critical infrastructure.

Area	Action/Requirement	Reference/Standard
Regulation & Procurement	Anchor on ISA/IEC 62443 for security measurability and enforcement	ISA/IEC 62443
Segmentation	Use zones-and-conduits	ISA/IEC 62443
Vendor Requirements	Require secure-by-design development and patchability	ISA/IEC 62443

Supplier Assurance	Mandate SBOMs, vulnerability disclosure, and support windows	ISA/IEC 62443
Operationalisation	Complete asset inventories, apply least-privilege network architecture, harden IT/OT interfaces, establish monitoring with anomaly detection, and rehearse incident response prioritising safety and availability.	NIST SP 800-82 Rev.3
Smaller Operators	Adopt CISA's Cross-Sector Cybersecurity Performance Goals as baseline (MFA, backups, logging, EDR where feasible, vulnerability and patch management), phase up to 62443 conformance	CISA, ISA/IEC 62443
Auditing & Testing	Targeted audits, safety-aware red-team exercises	
Compliance	Tie compliance to licensing and government procurement.	
Result	Balanced approach respecting OT safety constraints, straightforward controls, vendor accountability across critical infrastructure	

21. How could the 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?

Building a National View of Data Flows

Establish a Data Flow Observatory, a trusted mechanism for mapping and monitoring how sensitive data moves across the economy and internationally. Major industry players, including banks, telecommunications providers, cloud service providers, and data brokers, should submit periodic transparency reports. These reports, based on a standardized schema aligned with the voluntary data classification model, would disclose categories of data shared, purposes, retention periods, and cross-border transfers. Insights from the Observatory would integrate with existing national threat-sharing platforms, enabling early detection of unusual data flows and supporting proactive responses to malicious activity.

Enhancing Transparency and Provenance

To improve accountability, the government should require Data Bills of Materials (DBOMs) for high-value and sensitive datasets. A DBOM would serve as a supply-chain-style manifest that records dataset origins, lawful basis for collection, processing locations, consent mechanisms, and third-party access. This would enhance visibility into data handling practices across the ecosystem. Technically, provenance records embedded at the API layer would ensure traceability and allow for quick incident response when data misuse occurs.

Regulating the Data Brokerage Ecosystem

Data brokers represent a critical but opaque segment of the economy. To reduce risk without stifling legitimate analytics, the government should implement a national broker registry with licensing tiers. Brokers would disclose the types of data traded, security safeguards in place, and logs of law enforcement requests. Risk-based export controls and mandatory impact assessments for sensitive cross-border transfers would prevent data of national significance from being exploited by hostile actors. Enforcement should be guided by intelligence gathered through the Data Flow Observatory to ensure efficiency and proportionality.

Creating Secure Data Spaces

Innovation and security are not mutually exclusive. The government should partner with industry to create sector-specific data spaces in areas such as health, finance, energy, and transport. These environments would enable high-value data sharing under strict governance, using privacy-enhancing technologies such as differential privacy, secure multi-party computation, and confidential computing. Adoption can be incentivised by embedding these technologies in procurement requirements and grant programs, ensuring that secure-by-design principles are rewarded.

Improving Incident Reporting and Response

Incident reporting must generate actionable intelligence. Enhancements to the national cyber incident reporting portal should capture structured details on exfiltrated data classes, transfer paths, and broker involvement. This information would inform the Observatory and support no-fault reviews through the Cyber Incident Review Board. National playbooks should also be updated to address large-scale data breaches, with a focus on rapid takedown, containment, and coordinated victim notification.

Aligning Incentives and Reducing Burden

Policy measures must remain proportionate. Tiered obligations will ensure that large organisations deliver complete transparency while SMEs and not-for-profits use simplified templates supported by free tools. Safe harbors and limited-use protections should remain in place to encourage candid disclosures. The government can further support adoption by co-funding pilot projects in priority sectors, enabling approaches to be tested and refined before their wider rollout.

Measuring Outcomes

To ensure policies deliver impact, evaluation should focus on measurable outcomes rather than compliance burden. Key indicators could include reductions in unknown or opaque data flows, faster containment times for exfiltration incidents, adoption rates of classification frameworks and DBOMs, and the number of malicious transactions disrupted through data intelligence. These metrics would provide policymakers with a clear view of progress and identify areas that require further attention.

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?

1. **Codify what "proactive" means, with clear legal guardrails and safe harbors**
   Publish authoritative guidance on permissible proactive cyber defense activities, with model controls, notification pathways, and record-keeping standards. Link this to existing incident mechanisms so that lawful, good-faith defensive actions are protected by the limited use obligation, and feed lessons into the no-fault Cyber Incident Review Board.
2. **Use product standards and procurement to harden the attack surface**
   Leverage already delivered measures on smart device standards and labelling, the emerging code of practice for app stores, and the Technology Vendor Review Framework, then preference compliance in Commonwealth procurement and grants. Promote alignment with Quad Secure software principles to reduce software supply-chain risk.
3. **Make learning from incidents faster, richer, and safer**
   Enhance the Single Reporting Portal data model to capture technical indicators suitable for near-real-time blocking, while maintaining the legal protections that encourage candid reporting, and route anonymised findings to the Review Board for public learning.
4. **Institutionalise sector-wide resilience exercises**
   Expand the **CORIE model beyond finance** to other vital sectors by combining intelligence-led red teaming with cross-dependency playbooks and involving regulators to stress-test blocking at scale.
5. **Lower the cost of doing the right thing for SMEs and NFPs**
   Offer standard build packs, managed security blueprints, and voucher-style subsidies for EDR, email security, and secure browser controls, supported by the government's professionalization program for the cyber workforce.
6. **Simplify cyber regulation**
   Continue efforts to align obligations and streamline reporting via the single portal, maintaining security outcomes while decreasing compliance hurdles, allowing firms to reallocate expenses toward controls that directly lower risk.

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?

1. **Publish a conflict and crisis cyber RACI aligned with existing playbooks.**
   Define lead, support, and decision-making authorities for NOCS, ASD, sector regulators, and critical entities across the prepare, respond, and recover phases. Integrate with the nine sectoral playbooks already published and the remaining ones due, and anchor to the National Cyber Security Exercise Program cadence.
2. Conduct an annual national black swan exercise focused on systemic economic disruption. Organize a multi-sector, multi-jurisdiction simulation that tests cross-sector interdependencies, public communication strategies, and surge capacity of authorities. Build on the CORIE intelligence-led model used in finance to expand red teaming beyond a single sector.

3. **Exercise legal and policy rapid response levers.**
   Summarize the activation of preappointed authorities, cross-border cooperation, and sanctions coordination. Include rehearsals for utilizing the limited use obligation to expedite sharing during crises, and identify additional protections needed to help non-government entities block at scale.
4. **Drill end-to-end incident data flows.**
   Conduct a stress test on the Single Reporting Portal to handle high-volume intake and near-real-time distribution of operational indicators to defenders, with clear data fields for exfiltration scope and systemic risk indicators. Provide anonymized findings to the Review Board for quick public learning.
5. **Expand trusted group and ISAC participation under time pressure.**
   Use exercise injects to onboard and test additional sectors into trusted groups, building on the Health Cyber Sharing Network pilot, and publish simple join criteria and surge playbooks.

Shield 4 – Protected Critical Infrastructure

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

What works well. The SOCI framework is described as world-leading and has materially lifted the baseline, including alignment of telecommunications under SOCI, enhanced protection for business-critical data storage, activation of enhanced obligations for Systems of National Significance, and new crisis consequence powers. These changes strengthen clarity and capability across critical sectors.

Where SOCI falls short.

1. **Enforcement and assurance still maturing** – independent audits for Risk Management Programs and sector maturity evaluations are proposed but not yet in place, making assurance uneven.
2. **Obligation clarity gaps** – scope for Managed Service Providers and multi-tenant data storage remains unclear, leading to accountability gaps.
3. **Crisis response limitations** – frameworks do not yet enable real-time, economy-wide defensive actions or provide explicit legal protections for private sector blocking at scale.
4. **Telecommunications transition risks** – the integration of TSSR obligations into SOCI is still being finalized, with operational clarity developing.
5. **Regulatory overlap and fragmentation** – coexistence with other cyber and privacy regimes creates complexity and potential blind spots.
6. **International exposure** – cross-border risks, such as undersea cables and space assets, are not fully addressed within the domestic SOCI framework.
7. **Vulnerability disclosure gaps** – limited support for security researchers and inconsistent adoption of disclosure policies leave systemic weaknesses.

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

Cross border and shared infrastructure risks. The paper highlights the need to secure undersea cables and space assets in partnership with international

stakeholders, which extends beyond domestic SOCI settings and requires new cooperation mechanisms.

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

Partly. SOCI has shifted critical sectors toward outcome-based risk management; however, the Government proposes additional measures precisely to right-size the burden and improve assurance, including sector-specific maturity evaluations, closer collaboration among regulators to ensure efficient and right-sized oversight, and independent audits for Risk Management Programs. These proposals acknowledge that proportionality and consistency can be improved.

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

Workforce and capability uplift. Leverage Horizon 1 grants and the APS workforce plan as templates to co-fund industry training, simulation, and managed service blueprints, prioritising entities with systemic importance.

What Government's role should be. Set clear rules and crisis authorities, convene and fund shared infrastructure like CTIS and NCIP, provide practical guidance and model audits, simplify and harmonise overlapping obligations, and measure outcomes through consistent maturity and performance indicators.

Shield 5 – Sovereign Capabilities

39. What role should the 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?

Establish a National Cyber Security Reservist Program

- Create a structured cyber reservist corps, similar to military or emergency service reservists, where trained professionals from industry can be called upon during major incidents or national emergencies.
- Incentivise participation through tax benefits, paid leave arrangements co-funded with employers, and national recognition schemes.
- Leverage this pool during crisis response exercises, ensuring readiness and a whole-of-nation surge capability.

Attract and Retain Global Cyber Talent

- Designate cybersecurity as a priority occupation under the **National Talent Initiative Visa program**, with streamlined pathways for experts to live and work in Australia.
- Offer fast-tracked permanent residency for high-demand cyber roles such as threat intelligence analysts, penetration testers, and OT security engineers.

- Partner with global universities, research labs, and cyber centres of excellence to attract talent through fellowships and joint research placements.

Make Cyber Education More Accessible and Affordable

- Introduce education discounts and subsidies for cyber-related degrees, micro-credentials, and vocational programs, especially for SMEs, not-for-profits, and regional communities.
- Offer "study now, pay later" schemes linked to industry employment commitments, reducing upfront costs for students.
- Co-fund tailored training packages with industry associations to rapidly upskill existing IT and risk professionals into cyber roles.

Pilot Innovative Workforce Development Models

- **Apprenticeship and cadetship pilots** in critical infrastructure sectors, giving early-career professionals hands-on experience under senior supervision.
- **Rotational exchange programs** between government, industry, and academia to build cross-sectoral skills and mutual understanding.
- **AI-enabled training platforms** to simulate attack and defense scenarios, allowing scalable, cost-effective training across the workforce.

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

Defence and Intelligence

- Personnel with backgrounds in signals intelligence, electronic warfare, and operational planning bring analytic rigor, risk management, and incident response discipline. Many nations recruit ex-defence staff into SOCs and cyber threat intelligence functions.

Finance and Risk Management

- Professionals in compliance, fraud detection, and financial risk modelling bring quantitative and analytical skills relevant to threat detection, risk assessment, and governance.Financial services already operate under strong regulatory regimes, so familiarity with assurance and audit maps well to cyber governance roles.

Engineering and Operational Technology (OT)

- Electrical, industrial control, and systems engineers working with SCADA and OT environments have domain expertise critical for securing critical infrastructure.Their familiarity with safety-critical systems and risk management is directly applicable to industrial cyber defense.

Research

- **Australian Computer Society (ACS) Digital Pulse Reports**
- **US NICE Cybersecurity Workforce Framework**
- **UK Cyber Security Skills in the Labour Market report**

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?

1. Establish a National Cyber Research Priorities Council

- **Mandate**: Convene representatives from government, industry, academia, and think tanks to identify annual national cyber research priorities.
- **Scope**: Align priorities with the Cyber Security Strategy shields, for example safe technology, threat sharing and blocking, critical infrastructure protection, sovereign capability, and workforce development.
- **Deliverables**: Publish a rolling three-year research agenda, with annual refresh cycles and metrics aligned to the Strategy's evaluation framework.

2. Launch a Horizon 2 Cyber Research Grants Program

- **Challenge Grants (12–24 months):** Fast-cycle, priority-aligned projects to address identified gaps such as edge device security, privacy-enhancing technologies, and sector-specific resilience models.
- **Translational Hubs (24–36 months):** University-led, industry-embedded teams to accelerate research into deployable solutions, with commercialisation pathways.
- **Sovereign Capability Mini-Centres:** Niche but critical facilities, for example red-team labs, incident analysis environments, and sovereign chip or cloud security research.
- **Workforce and Methods Grants:** Datasets, open architectures, educator fellowships, and professionalisation programs that build the next generation of cyber expertise.

3. Reduce Collaboration Friction

- Standardised collaboration agreements covering IP, data use, and publication to cut transaction costs.
- Secure, government-funded testbeds and privacy-preserving environments for real-world data analysis.
- Consortia eligibility requirements, with each project including at least one university, one industry partner, and one government end-user.
- Rolling quarterly grant intakes, to ensure agility and inclusion.

Shield 6 – Strong Region and Global Leadership

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

Shortlist of regulatory frameworks and requirements that Australia should prioritise for international alignment, mapped to Strategy Horizon 2 focus areas and existing Horizon 1 actions.

International Cyber Regulatory Alignment – Priority Matrix

Domain	Peer Frameworks to Align With	Benefit for Australia
Incident & ransomware reporting	EU NIS2 Directive, US CIRCIA, UK incident rules	Consistent reporting fields & timelines, streamlined global compliance, faster cross-border threat response
Consumer & edge product security	EU Cyber Resilience Act, Singapore IoT labelling, UK PSTI Act	Ensures Australian device standards & labels are interoperable globally, boosts consumer trust & export readiness
Secure software development & procurement	Quad secure software principles, US Executive Order 14028	Reduces supply chain risk, aligns government procurement with allies, lifts vendor assurance
Threat intelligence sharing & blocking	US CISA JCDC model, UK NCSC CiSP, EU CSIRTs Network	Enables real-time indicator exchange, supports ISPs/telcos in scaling blocking, and strengthens collective defence
Critical infrastructure assurance	US CIRCIA, UK NIS2, EU DORA (for finance)	Comparable maturity assessments & independent audits, clearer cross-border interdependencies
Data security & cross-border governance	EU GDPR, Singapore PDPA, US NIST data frameworks	Harmonises retention & brokerage rules, reduces regulatory friction for multinational firms
Cybercrime cooperation	UN Cybercrime Convention, Budapest Convention	Faster evidence sharing & mutual legal assistance, stronger global deterrence
Post-quantum cryptography	US NIST PQC standards, EU ENISA roadmap	Coordinated adoption timeline, avoids fragmentation, secures trade & defence supply chains
Sanctions & counter-ransomware	US/UK sanctions regimes, Counter Ransomware Initiative	Aligned disruption & deterrence, unified global response to ransomware actors
App store & platform safety codes	EU Digital Services Act, UK Online Safety Act	Improves app ecosystem security, protects Australian consumers, aligns developer obligations