Check Point Australia

Response to Appendix A Questions for HORIZON 2

Prepared by:

Check Point Australia

Check Point Software Technologies [Australia] Pty Ltd.

[redacted]

[redacted]

Point of Contact:

[redacted]

[redacted]

Australia & New Zealand

[redacted]

2. Developing our vision for Horizon

2 2.1 Outlook for Horizon 2

Question 1

What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?

Australia's cyber outlook over the next decade will be shaped by the accelerating adoption of artificial intelligence, quantum computing, the growth of connected devices, and the transition to 6G networks. These developments will drive innovation but also expand the threat surface dramatically. Adversaries are already leveraging AI to automate attacks and generate realistic phishing, while defenders must ensure resilience, transparency, and security-by-design. Without early preparation, the national transition to post-quantum cryptography risks fragmentation and systemic vulnerabilities, as adversaries seek to exploit lagging sectors.

The strategic factors for Horizon 2 will need to focus on:

- **Proactive Cybersecurity:** Promote active cyber defense (ACD) and scale threat-blocking capabilities.
- **Regulatory Simplification:** Harmonize domestic regulations and align with global standards.
- **Workforce Development:** Expand programs like the Cyber Workforce Playbook and target diversity.
- **Public-Private Collaboration:** Strengthen partnerships for threat intelligence sharing and co-develop solutions.
- **Emerging Tech Security:** Focus on AI, quantum, and IoT security with security-by-design principles.
- **Regional Leadership:** Enhance engagement with Southeast Asia and the Pacific through initiatives like SEA-PAC Cyber.
- **Data Protection:** Strengthen privacy policies and expand Digital ID use.
- **Crisis Preparedness:** Conduct cyber exercises and develop scalable incident response frameworks.

In addition, this plan must also recognise the increasing dependency of households and industries on digital services, with the average Australian home expected to host over 30 connected devices by 2027. Critical supply chains add further complexity and exposure, demanding stronger baseline protections and sector-specific resilience measures. In this environment, adopting a prevention-first and intelligence-led posture is essential. National cyber exercises, stress-testing of recovery frameworks, and a cyber reserve capability to provide surge support during crises will help close capability gaps.

Equally important is workforce uplift. Expanding practical training, apprenticeships, and lateral entry programs will address the growing shortage of skilled professionals. By embedding prevention, intelligence sharing, and workforce resilience into this plan, Australia

can build an adaptive and trusted cyber posture—capable of protecting national interests, critical infrastructure, and citizens in an increasingly contested digital environment.

2.2 Collaborating across all levels of Australian Government

Question 2

Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?

Several state-led initiatives offer strong foundations that could be scaled nationally. Cyber security awareness campaigns such as *"Act Now. Stay Secure"* demonstrate the value of concise, action-oriented messaging. Expanding this program across all levels of government would ensure consistent, credible communication, helping individuals and small businesses take practical steps against real threats. Similarly, state-driven workforce initiatives, including STEM engagement and mid-career transitions into cyber security, should be elevated to a national scale to expand the talent pipeline and address the skills shortage.

Threat intelligence pilots also highlight the potential for national replication. For example, the Health Cyber Sharing Network (HCSN) demonstrates how sector-specific intelligence exchanges improve situational awareness and preparedness. Extending this model into other critical sectors such as energy and transport could deliver a unified, cross-sector approach to intelligence-led resilience.

Finally, state programs focused on strengthening critical infrastructure—particularly in energy and transport—have shown value and could be replicated federally. This would reduce fragmentation and ensure all operators meet consistent resilience standards. By harmonising successful state-level campaigns, training, and sharing networks into a national framework, this plan can deliver a cohesive and scalable approach to awareness, intelligence, and resilience across Australian society.

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

Question 3

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

The high-level model outlined in this plan provides a valuable foundation for evaluating outcomes. Its structured approach—defining objectives, linking interventions, and embedding metrics does align well with the need for a dynamic and responsive cyber security strategy. However, refinement is needed to ensure future relevance. The model should explicitly account for risks emerging from artificial intelligence, quantum computing, and IoT, embedding them as priority domains. Sector-specific metrics must also be introduced, recognising the distinct needs of critical infrastructure operators, SMBs, and NFPs.

Feedback mechanisms are critical. Real-time data collection and feedback loops will allow adjustments to be made quickly as threats evolve. Incorporating internationally recognised frameworks such as VERIS would also standardise reporting and align Australia's datasets with global peers. Finally, the model must remain accessible. Simplified reporting tools and plain-language communication will help SMBs, NFPs, and boards engage meaningfully.

Measuring the strength of public-private collaboration should also be built into the framework, ensuring partnerships contribute to resilience. With these refinements, the model can remain adaptive, intelligence-led, and outcome-focused—capable of guiding both government and industry toward a prevention-first posture.

Question 4

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

Monitoring outcomes requires combining structured incident data with insights from real-world activity. International taxonomies such as VERIS provide a strong basis, enabling consistent classification and global comparability. This should be complemented by enhanced mandatory reporting across industries—not limited to ransomware payments—so government has visibility of a broader range of incidents.

Threat intelligence platforms such as the Cyber Threat Intelligence Sharing (CTIS) system can be leveraged for real-time adversary data, supported by structured feedback from industry forums and partnerships like the National Cyber Intel Partnership. Lessons learned from

cyber exercises (e.g., CORIE) should also be systematically captured to identify capability gaps and refine interventions.

Regular maturity surveys and independent audits would provide a complementary view of organisational preparedness, while anonymised user-behaviour analytics (such as MFA adoption or passwordless uptake) could help measure public progress. Importantly, the government should establish accessible feedback portals for citizens and businesses to report challenges and provide input. Combined with academic longitudinal studies, this will deliver a layered, intelligence-led understanding of progress.

By integrating structured frameworks, threat intelligence, exercises, and stakeholder feedback, this plan can ensure that monitoring is both comprehensive and responsive to evolving risks.

3. Shield-level focus for Horizon 2

3.1 Shield 1: Strong businesses and citizens

Question 5

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

Cyber awareness campaigns are most effective when they are intelligence-led, targeted, and action-oriented. This plan should consolidate resources into a unified national platform, providing clear, practical guidance to households, SMBs, and NFPs. Rather than generic warnings, campaigns must address the threats Australians face daily—phishing, scams, ransomware, and identity crime—using current data to drive credibility.

Tailoring messages to different demographics is critical. Younger Australians engage via TikTok and Instagram, professionals through LinkedIn, and parents via mainstream media. Aligning campaign delivery to these consumption patterns maximises impact. Public-private partnerships can further extend reach, with banks, telcos, and ISPs amplifying messages through trusted channels. A unified messaging platform could be helpful to centralise all cyber awareness resources on a single, user-friendly platform for consistent messaging and easy access.

Successful campaigns such as *"Act Now. Stay Secure"* should serve as a template: concise, relatable, and directly linking actions (e.g., enabling MFA, using passkeys) to the threats they mitigate. Integrating cyber literacy into education ensures longer-term awareness and embeds safe habits early.

Finally, government messaging should harmonise with industry rollouts of new security features, working with state and local governments, ensuring the public understands why controls are changing and how they protect. By consolidating platforms, tailoring outreach, and amplifying through partnerships, this plan can deliver a trusted, consistent national awareness message that drives measurable uplift.

Question 6

What programs or pilots have been successful in this context? What additional supports could be developed or scaled up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?

Several domestic and international pilots have demonstrated the power of education, collaboration, and practical exposure. In Australia, school-based STEM and digital literacy programs have successfully introduced cyber concepts early, while campaigns such as *"Act Now. Stay Secure"* have shown the value of concise, action-oriented messaging.

Internationally, the UK's *CyberFirst* and the US *CISA School Partnerships* illustrate how camps, mentoring, and structured engagement can build long-term pathways into cyber careers.

This plan should build on these successes by scaling national cyber literacy programs across schools especially embedding AI-awareness into the curricula, integrating both technical skills and awareness of AI risks eg. AI-driven misinformation and scams. Teacher training and curriculum support will be essential to embed cyber education sustainably. Partnerships with industry should expand mentorship, internships, and scholarship opportunities, particularly for underrepresented groups such as women, First Nations people, and culturally diverse communities.

Gamified tools, interactive platforms, and targeted advertising across social and mainstream channels can also make cyber concepts accessible to different demographics. By combining education, technical expertise, and community outreach, this plan can ensure Australians are not only aware of cyber risks but empowered with the skills to counter them.

Question 7

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

SMBs and NFPs face unique constraints—limited budgets, competing priorities, and minimal technical expertise. To overcome these barriers, this plan should simplify access to resources by consolidating them into a central, user-friendly platform with clear, jargon-free guidance tailored to smaller organisations. Awareness campaigns, amplified through local chambers of commerce and industry associations, can promote these resources through trusted channels.

Financial incentives remain critical. Targeted grants, subsidies, or tax relief tied to the adoption of essential cyber practices—such as MFA, backups, or Cyber Wardens participation—would reduce cost barriers and demonstrate government recognition of their challenges. Recognition programs, such as certificates or public registers for resilient organisations, could also build trust with donors, customers, and partners. Providing free or low-cost training programs, workshops and personalized support to help SMBs and NFPs is another means to encourage these groups to implement cyber security practices.

Finally, expanding training and one-on-one support, delivered through public-private partnerships, would provide SMBs and NFPs with practical guidance to implement measures effectively. By reducing complexity, offering incentives, and embedding support within existing business networks, this plan can ensure that smaller organisations—often the backbone of our economy and community—are better protected against cyber threats.

Question 8

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

Collaboration between government and industry is essential to overcome barriers faced by SMBs and NFPs. This plan should prioritise joint initiatives that are practical, sector-specific, and financially supported. Public-private partnerships can co-develop simplified frameworks tailored to smaller organisations, while industry associations can act as trusted intermediaries for awareness and outreach.

Government should incentivise adoption through grants, tax concessions, or subsidised cyber security tools and services, while industry contributes expertise, training, and affordable bundled solutions. Recognition programs and certifications would provide credibility, enhancing trust among customers and donors. Real-time threat intelligence platforms could also be extended to include smaller organisations, ensuring they receive timely warnings and practical guidance.

Crucially, compliance expectations should be proportionate. Streamlined regulatory requirements, aligned with broader national standards, would ensure SMBs and NFPs can focus on meaningful action rather than administrative burden. By embedding joint campaigns, shared intelligence, and sector-specific frameworks into this plan, government and industry can together uplift the maturity of smaller organisations, closing a critical resilience gap across the national economy.

Question 9

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

Practical, accessible standards are essential for SMBs and NFPs. The Australian Signals Directorate's *Essential Eight* provides a strong baseline, enjoying critical mindshare across executives, boardrooms and the community in general, but a simplified, tiered version would make adoption more achievable for smaller organisations. Globally, frameworks such as ISO/IEC 27001, the NIST Cybersecurity Framework, and the UK's *Cyber Essentials* offer scalable pathways that could be adapted locally. For payment-focused entities, PCI DSS (Payment Card Industry Data Security Standard) remains critical for secure transactions. Emerging IoT and sector-specific standards must also be considered.

The Government's role should be to endorse and harmonise these standards acting as bridge and enabler, ensuring they are open, affordable from recognised standards bodies (like OASIS) or government agencies, and not locked behind costly "pay-to-play" models.

Support should include free tools, templates, and implementation guidance, particularly for low-maturity organisations. Certification pathways, whether simplified badges or sector-specific recognition, can build confidence and trust.

By reducing cost and complexity, aligning with international norms, and tailoring standards to local needs, this plan can ensure smaller organisations uplift their resilience in a consistent, nationally coherent manner.

Question 10

What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?

Not-for-profits face distinct challenges that leave them disproportionately exposed. Many operate with limited budgets, high staff turnover, and reliance on volunteers who may not receive consistent training or have the relevant cyber knowledge to stay safe. At the same time, NFPs often hold highly sensitive beneficiary and donor data, making them attractive targets for cybercriminals. The reputational damage from a breach can be especially severe, undermining public trust and donor confidence.

Government interventions should be targeted to these realities. Grants, subsidies, or free access to essential cyber security tools could directly offset resource constraints. Training programs designed for non-technical staff and volunteers would provide practical, sustainable uplift. Simplified standards and checklists tailored to NFP needs can ensure core controls—such as MFA, backups, and incident response planning—are achievable without unnecessary complexity.

Government-backed rapid response support for incidents would also be highly valuable, ensuring NFPs are not left to recover alone. Expanding the existing Cyber Resilience and Cyber Warden programs, may include a clear definition of what controls are expected when collecting certain data, creating a dedicated portal with tools and guidance for NFPs to improve their security posture and establishing a government-backed rapid response team to assist NFPs in managing and recovering from cyber incidents would also be helpful. Finally, public recognition for resilient NFPs could strengthen donor confidence and encourage adoption of stronger practices. By tailoring interventions to the realities of NFPs, this plan can safeguard both critical community services and the Australians who depend on them.

Question 11

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

Cyber insurance has become increasingly difficult for SMBs and NFPs to access. Rising premiums due to rising cyber threats making it less affordable, complex eligibility requirements, and limited awareness of coverage are creating significant barriers. Many policies are designed with large enterprises in mind and impose compliance prerequisites—such as stringent patching, MFA, and 24/7 monitoring—that smaller entities may lack the capacity to meet. Even when policies are purchased, exclusions and complex clauses can lead to uncertainty, undermining confidence in their value.

For smaller organisations with limited resources, the cost of premiums often outweighs their perceived risk, particularly when they are unclear about what incidents are actually covered, with some insurance companies avoiding payment after an incident. This leads to underinvestment in both insurance and preventative controls, leaving critical gaps in resilience.

To address these challenges, this plan should encourage insurers to develop simpler, low-cost products tailored to the needs of SMBs and NFPs. Subsidies, pooled risk models, or group policies coordinated through industry associations could improve affordability. Awareness campaigns, combined with access to free or subsidised cyber risk assessments, or discounts on premiums for companies demonstrating strong cyber measures would also help organisations understand both their risk exposure and the role of insurance in complementing preventative measures.

By addressing affordability, clarity, and accessibility, this plan can ensure that cyber insurance becomes a meaningful tool for resilience, not a barrier to entry.

Question 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 significant and evolving threats to individuals and small entities. For SMBs and NFPs, limited budgets and cyber expertise and defenses make them attractive targets, with attacks often causing operational disruption, reputational damage, and financial loss. Attackers increasingly employ double and triple extortion models—encrypting data, threatening to leak it, and targeting customers or partners. Ransomware-as-a-Service (RaaS) has lowered barriers to entry, enabling even low-skilled actors to launch sophisticated campaigns.

Individuals are not usually the primary target but are increasingly affected through identity theft, fraud, and extortion following breaches of larger organisations that hold personal data. Vulnerable groups, including older Australians and those less digitally literate, remain disproportionately at risk. Attackers are demanding larger ransoms, often in cryptocurrency, making recovery more expensive, especially as attackers target the critical infrastructure sector, amplifying the societal impact, forcing payment to the attackers.

The threat is evolving through automation and the use of AI, which allows adversaries to scale phishing and reconnaissance with greater precision, though harder to detect. Globally, ransom demands are increasing in both frequency and cost, and sectors such as healthcare, education, and NFPs face rising targeting due to their reliance on sensitive data and lower cyber maturity.

For policymakers, this highlights the urgent need for prevention-first strategies, practical support for smaller entities such as low-cost or free tools for ransomware prevention, and international cooperation to disrupt ransomware groups. Without proactive intervention, the scale and impact of ransomware will continue to grow.

Question 13

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

Protecting against ransomware requires a layered and prevention-first approach. For SMBs and NFPs, government support should focus on making essential defences both accessible and affordable, especially as the cost of a cybersecurity incident can vastly outweigh the cost of foundational preventative measures. Subsidised access to endpoint protection, backup solutions, and firewalls would provide a baseline layer of defence. Complementing this, simple guidance tailored for smaller entities should set out clear, achievable steps such as MFA adoption, patching routines, and offline backups.

Public awareness campaigns must continue to highlight common attack vectors, particularly phishing and social engineering, while providing practical advice that resonates with individuals and small business owners. Campaigns should move beyond traditional advertising to include contemporary communication methods—such as targeted social media messaging and integration into mainstream entertainment—to reach diverse audiences.

Mandatory reporting regimes for ransomware incidents and payments should be strengthened, providing the government with data to inform policy and help disrupt adversaries. Rapid-response support services, including government-backed hotlines and recovery teams, minimum cyber security standards for small businesses handling sensitive

data and sharing of ransomware threats could also help businesses and individuals contain and recover from attacks more effectively.

By combining financial incentives, accessible tools, intelligence sharing, and novel awareness methods, this plan can reduce the prevalence of ransomware incidents and improve the resilience of both organisations and individuals.

Question 14

Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?

Certain communities and sectors face disproportionate impacts from cyber incidents due to resource constraints, digital literacy gaps, or reliance on sensitive data. SMBs and NFPs often operate with limited budgets and expertise, leaving them vulnerable to phishing, ransomware, and data theft. For NFPs in particular, with their reliance on volunteers, working on usually outdated systems and sensitive donor data, a single breach can significantly erode donor trust and disrupt essential services.

Vulnerable individuals—including older Australians, First Nations people, and people with disabilities—may lack access to tools, education, or support, making them easier targets for scams and identity theft. Similarly, the healthcare sector faces heightened risks due to high-value patient data and reliance on legacy systems, with breaches carrying both financial and safety implications.

The impacts extend beyond financial loss, often affecting trust, mental health, and community wellbeing. For example, identity theft can create long-term credit and reputational issues for individuals, while small businesses may struggle to recover from prolonged operational disruptions.

Addressing these vulnerabilities requires tailored interventions: targeted awareness campaigns for vulnerable demographics, subsidised support for SMBs and NFPs, and sector-specific resilience programs for healthcare and education. By focusing resources where harm is greatest, this plan can close equity gaps in cyber resilience and ensure protection is distributed fairly across society.

Question 15

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

Support services for victims of identity crime must shift from today's fragmented, victim-led approach to a coordinated, systemic framework that embeds responsibility across

government, industry, and breached organisations. Currently, obligations on organisations that suffer a breach are minimal, often limited to notification, leaving individuals to shoulder the complex and stressful process of recovery alone. Legislative reform should establish clear requirements for breached organisations to fund recovery services — including counselling, credit monitoring, financial advocacy, and legal support — either directly or through trusted providers such as IDCare. This ensures victims are not left to manage the consequences in isolation and that the cost of recovery sits with those whose security failures caused the harm.

Technology and government-backed platforms also have a critical role to play. Services such as MyGov Digital Verification Service (DVS) could be expanded to reduce the need for widespread collection and storage of sensitive identity documents, minimising exposure risk across the economy. MyGov could also introduce identity "lockdown" features, similar to credit freezes, allowing victims to restrict use of compromised credentials across institutions. Organisations would be legally obliged to honour these restrictions. In parallel, a breach-victim recognition feature could help individuals prove compromised status, enabling fair treatment when accessing services affected by fraud-related credit issues.

Accessibility and efficiency should underpin design. A centralised support hub would act as a one-stop portal for victims to report crimes, access resources, and receive step-by-step recovery guidance. This should be supported by government-backed rapid response teams to secure accounts, freeze credit, and restore identities, alongside proactive notifications from tools like the Identity Verification Services Credential Protection Register to alert victims when their data is misused.

Crucially, support must be tailored. Vulnerable groups such as the elderly, First Nations people, and individuals with disabilities face unique barriers and must have equitable access to recovery services. Public awareness campaigns, combined with industry collaboration — particularly with banks, telcos, and technology providers — can further strengthen fraud detection, accelerate victim support, and improve prevention.

Finally, identity crime is not only a financial problem but also an emotional one. Fraudulent activity can impact large life events like securing a mortgage, but also everyday situations such as booking a hotel or making an online purchase. Recognising these wider consequences underscores the importance of holistic recovery services.

In short, an effective framework must:

1. Mandate breached organisations to fund victim recovery services.
2. Expand government-backed platforms like MyGov to minimise exposure and provide lockdown features.
3. Deliver centralised, streamlined, and proactive support tools.
4. Ensure tailored assistance for vulnerable groups.

5. Acknowledge both the financial and emotional consequences of identity crime.

By combining legislative reform, practical government-backed safeguards, and collaborative industry engagement, victims will be supported in a way that is timely, humane, and sustainable — with the financial burden carried by those responsible for the breach, not the individuals harmed.

Question 16

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

Reducing systemic cyber risk requires a regulatory approach that is prevention-first, intelligence-led, and grounded in accountability. Strengthening audit standards, clarifying directors' responsibilities, and enforcing data minimisation and deletion obligations would meaningfully reduce the harm Australians face during ransomware or data theft incidents. Several existing frameworks provide a strong foundation. The *Security of Critical Infrastructure (SOCI) Act* establishes essential obligations for critical sectors, but its effectiveness depends on consistent enforcement and proportionate application across industries. *Prudential Standard CPS 234* ensures resilience within financial services, while the *Privacy Act* (including mandatory breach notification) underpins consumer protection by requiring organisations to safeguard personal information.

Emerging reforms, such as the *Cyber Security Act 2024* mandating baseline controls for smart devices and ransomware payment reporting, are also vital to address evolving threats. Today, frameworks like APRA CPS 234 and the Security of Critical Infrastructure (SOCI) Act require entities to manage cyber risks and test security controls, but they stop short of mandating intelligence-driven, adversary-emulation exercises. Collectively, these frameworks create a patchwork of defences; however, greater harmonisation is needed to reduce overlap and complexity.

International best practice shows the importance of embedding *Intelligence-Led Red Teaming (ILRT)* requirements, as seen in the UK's CBEST and Europe's TIBER-EU programs. Singapore and Hong Kong require ILRT for major financial services institutions through their iCAST programs. Mandating ILRT for critical sectors would ensure organisations are tested against real adversary tactics, not just compliance checklists.

The most important regulations in reducing cyber risk in Australia are those that improve transparency, accountability, and resilience across critical sectors. The Mandatory Data Breach Notification Scheme plays a central role by requiring organisations to notify both regulators and affected individuals of significant breaches, ensuring victims can take protective steps and incentivising stronger data security practices. The Ransomware Payment Reporting Regime is equally vital, as it builds a clearer national picture of

ransomware activity — including frequency, sectors targeted, and amounts paid — enabling policymakers and law enforcement to deliver more targeted responses and coordinate internationally. Finally, the Telecommunications Sector Security Reforms (TSSR) align telcos with critical infrastructure standards, ensuring Australia's communication networks remain resilient against both criminal and state-based threats.

Australia could map to this international direction by embedding TIBER-EU–style ILRT requirements into CPS 234 and SOCI. This would ensure that financial institutions and critical infrastructure providers are continuously tested against credible threat scenarios, closing the current assurance gap.

By combining prevention-first obligations, stronger director accountability, and threat-informed assurance mechanisms such as ILRT, this plan can significantly reduce systemic cyber risk, improve consumer trust, and align Australia with global leaders in cyber regulation.

Question 17

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

At Check Point, regulatory requirements have not negatively impacted our own cyber maturity. However, as a cyber security provider working with organisations across Australia, we regularly observe how compliance obligations can create challenges that hinder genuine resilience. Too often, requirements are interpreted as "checklists," diverting resources towards documentation and audit preparation rather than proactive security. This can result in a posture that looks strong on paper but lacks the ability to withstand real-world adversaries.

The complexity and overlap of frameworks — such as the SOCI Act, CPS 234, and the Privacy Act — also create duplication of effort and unnecessary administrative burdens. Smaller organisations in particular face significant strain, with one-size-fits-all obligations that are costly and difficult to implement. In some cases, limited budgets and expertise force SMBs and NFPs to prioritise compliance reporting over investments in proactive defence measures.
We believe the most effective way to manage these issues is to take a threat-informed, prevention-first approach.

Mapping compliance requirements to frameworks such as MITRE ATT&CK, adopting Intelligence-Led Red Teaming (ILRT) practices like TIBER-EU, and aligning with pragmatic frameworks such as the Essential Eight, ensures that regulatory obligations are met while controls remain effective against real adversary behaviours. Streamlining compliance through automated reporting tools, engaging with industry groups and regulators for clearer guidance, and investing in staff training further help organisations balance compliance and security.

Ultimately, regulatory frameworks should incentivise outcome-based resilience rather than documentation-heavy compliance. By harmonising overlapping requirements, offering tailored guidance for smaller entities, and embedding technical clarity on “what good looks like,” Australia can uplift compliance in a way that strengthens genuine operational maturity rather than undermining it.

3.2 Shield 2: Safe technology

Question 18

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

Internationally, several frameworks demonstrate strong approaches to securing emerging technologies. For edge devices and IoT, the *EU Cyber Resilience Act* and ETSI EN 303 645 establish mandatory secure-by-design principles, including strong access controls, secure update mechanisms, and vulnerability disclosure processes. Singapore's *Cybersecurity Labelling Scheme* further empowers consumers to make informed choices.

For consumer energy resources (CER), Europe's *NIS2 Directive* and Network Codes on Cybersecurity for Electricity Transmission emphacise proactive risk management, incident reporting, and resilience testing—practices directly relevant to Australia's energy transition.

For operational technology (OT), Europe's *TIBER-EU* framework shows the value of intelligence-led red teaming to test resilience against adversary behaviour. Combined with NIS2's high-level OT guidance, this ensures operators not only comply with standards but actively enhance resilience, reducing the likelihood that attacks on industrial or critical systems impact consumers. Singapore's Critical Information Infrastructure framework also provides a robust governance model.

This plan should adopt a prevention-first approach by mandating secure-by-design principles for devices, sector-specific resilience standards for CER, and ILRT requirements for OT operators.

Aligning with proven international standards will ensure consistency with allies, protect consumers, and strengthen critical infrastructure. By embedding security at the design stage and validating resilience through adversary simulation, Australia can achieve a higher baseline of trust in its technology ecosystem.

Question 19

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

Consumers face increasing exposure through insecure products and services, often without the tools or knowledge to protect themselves. This plan should prioritise transparency, regulation, and education to shift responsibility away from individuals managing insecure systems and toward ensuring products are secure by default.

A national product labelling or certification scheme, aligned with international models such as Singapore's *Cybersecurity Labelling Scheme*, would allow consumers to easily identify products meeting baseline standards. Public awareness campaigns can then explain how features such as automatic updates, strong authentication, and vulnerability reporting protect end-users in practical terms.

Government should also expand collaboration with manufacturers and retailers to include guidance at the point of sale, ensuring consumers receive security information when it is most relevant. For households, subsidised access to simple tools such as password managers, antivirus software, and backups would further reduce barriers.

Finally, accessible reporting channels for suspected vulnerabilities or scams should be established, empowering consumers to act safely. By combining secure-by-design regulation, transparent labelling, and practical guidance, this plan can help Australians make informed choices, improve trust in digital products, and reduce the likelihood of consumer harm.

Question 20

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

Clearer and more actionable guidance would help organisations assess and mitigate foreign ownership, control, or influence (FOCI) risks effectively. Currently, ambiguity creates uncertainty in procurement and risk management.

This plan should establish a national risk assessment framework, with standardised criteria for evaluating vendor ownership structures, affiliations, and potential security threats. A government-managed vendor risk database, providing transparent risk ratings, would simplify decision-making and avoid duplication across sectors.

Approved vendor lists for critical technologies could provide further assurance, particularly in areas such as telecommunications, healthcare, and energy. Government should also develop sector-specific guidance, recognising the unique risk profiles of different industries.

Training programs and workshops would help organisations understand how to identify and mitigate FOCI risks, while a central reporting mechanism could enable businesses to raise concerns and share intelligence. For SMBs, simplified tools and templates would prevent undue burden while ensuring national consistency.

By providing clear frameworks, transparency, and practical support, this plan can help organisations make informed procurement decisions, reduce systemic risk, and align security requirements with national interest.

Question 21

How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors? Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft).

Secure and trusted data sharing is essential to innovation, but today it remains fragmented and often poorly understood. Organisations face uncertainty over which data must remain sovereign, how cross-border transfers should be managed, and what constitutes adequate protections. This ambiguity creates compliance challenges and exposes gaps that malicious actors can exploit. Guidance on exportable data should specify conditions for secure transfer, including encryption, third-party vetting, and adherence to local and foreign regulatory requirements. The government could also mandate periodic audits or reporting of long-term data storage, ensuring organisations are aware of what data they retain and reducing the potential impact of breaches.

This plan should establish a joint government–industry taskforce to map data flows across the economy and identify systemic risks. A national framework should then set out clear definitions of sovereign and sensitive data, sector-specific storage requirements, and minimum safeguards for transfers. Encryption, anonymisation, and third-party vetting must be embedded as baseline expectations.

Incentives such as tax relief or certification could reward organisations adopting trusted data-sharing practices. Meanwhile, sector-specific platforms—such as health data exchanges—can provide controlled environments that balance innovation with protection. Government should also promote advanced technologies, such as blockchain and Digital ID, to reduce reliance on high-risk data collection. Collaboration between government and industry could include shared intelligence on emerging threats to data transfers, workshops on secure data architectures, and the development of standardised frameworks for risk-based, controlled data sharing, enabling organisations to balance innovation with strong safeguards against exploitation.

By combining clarity, practical frameworks, and shared responsibility, this plan can ensure data is shared with trust, limiting exploitation while enabling economic prosperity.

Question 22

How does Government and Industry work together to achieve this aim in an evolving global threat environment?

Protecting Australian innovation and enabling trusted data sharing requires a prevention-first, intelligence-led approach anchored in strong collaboration between government and

industry. Malicious actors are increasingly targeting intellectual property, R&D data, and sensitive commercial information, yet many organisations still underestimate the sophistication of these threats. Addressing this requires a coordinated model where government provides transparency on the scale, nature, and methods of IP theft, while industry contributes operational insight into incidents and adversary behaviours.

Stronger public–private partnerships (PPPs) are central. These should include shared intelligence platforms, secure briefings on emerging adversary tactics, and joint task forces to coordinate policy and operational responses. Timely, anonymised threat intelligence from government would allow companies to adopt proactive measures, while industry's contribution of incident data would enhance national situational awareness. Together, this dual flow of intelligence strengthens resilience across the economy.

Equally important is the co-design of standards and policies. Jointly developed frameworks for secure data governance, cross-border transfers, and risk-based operational practices will help balance the twin priorities of innovation and security. Alignment with international norms and standards is also critical to support trade and compliance in a globally connected economy.

Practical collaboration should extend into joint cyber exercises across critical and strategic sectors — including healthcare, research, and manufacturing — simulating adversary campaigns against intellectual property to test resilience and close gaps. Government can also incentivise investment in protective controls through grants, tax concessions, and R&D funding, while industry invests in secure technologies, security-by-design practices, and workforce training. Initiatives to build a skilled cyber workforce, such as scholarships, apprenticeships, and mid-career transition programs, should be co-funded and co-delivered.

Finally, international cooperation is essential. By working with allies on norms, sanctions, and rapid takedowns of malicious infrastructure, Australia can raise the operational costs for adversaries while protecting its innovation ecosystem. Public awareness campaigns co-branded by government and industry will also reinforce a culture of shared responsibility, empowering citizens and businesses to strengthen resilience at every level.

In short, by combining intelligence sharing, co-designed standards, joint exercises, incentives for investment, and global alignment, government and industry can create an environment where data is shared with trust, innovation is safeguarded, and Australia's economic prosperity is secured in an evolving global threat landscape.

Question 23

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

Emerging technologies such as AI, quantum computing, and IoT will transform society, but without safeguards they risk creating systemic vulnerabilities. This plan should prioritise practical, prevention-first guidance that enables safe adoption while maintaining public trust.

Clear frameworks for technology adoption are essential. The Government should publish frameworks for assessing risks associated with new technologies, setting clear expectations for privacy, resilience, and ethical use as well as strong data governance and transfer standards. Secure-by-design principles must be mandated, with minimum standards for encryption, patching, and software integrity embedded into devices and platforms. A regulatory “sandbox” model could allow organisations to test emerging technologies in controlled environments before large-scale deployment.

Practical tools—such as risk assessment checklists, templates for secure AI development, and guidance on quantum-resistant cryptography—should be made accessible to organisations of all sizes. At the same time, government should fund R&D into security innovations, particularly around quantum, AI, and data governance, and promote public awareness of emerging risks such as deepfakes or AI-driven misinformation through regular briefings, sector-specific case studies and anonymized threat intelligence.

Finally, international collaboration is vital. Aligning Australia’s standards with global frameworks (such as GDPR, NIST, or international AI ethics principles) will not only safeguard against threats but also position Australia as a competitive, trusted leader in secure technology adoption.

By embedding clear standards, supporting innovation through safe testing, and empowering organisations with practical tools, this plan can ensure that Australia harnesses the benefits of emerging technologies without compromising security or public confidence.

3.3 Shield 3: World-class threat sharing and blocking

Question 24

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

A proactive posture requires moving beyond compliance to continuous, intelligence-led defence. Too often, organisations focus on minimum regulatory requirements rather than resilience against real adversaries. This plan should embed prevention-first and intelligence-informed practices as the national standard.

The Government can support this by establishing trusted intelligence-sharing networks, providing timely, anonymised insights into adversary tactics that industry can operationalise. Building on the National Cyber Intel Partnership (NCIP) and Cyber Threat Intelligence Sharing (CTIS) platform, the government can encourage broader participation and provide incentives for industries to share actionable intelligence. Guidance should prioritise secure-by-design principles, threat-informed vulnerability management, and active defence measures that reduce harm before incidents occur. Financial incentives and procurement levers should reward organisations that demonstrate validated resilience, not just compliance.

For industry, a proactive posture means adopting cyclical practices—regular red teaming, resilience testing, and intelligence-informed control validation—rather than static controls. It requires embedding adversary-informed playbooks, investing in secure-by-design engineering, and maintaining continuous improvement through lessons learned.

Australia's proactive posture should therefore be outcome-focused, constantly tested, and intelligence-led, underpinned by open collaboration between government and industry. This approach will ensure national resilience keeps pace with evolving threats.

Question 25

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

Rather than creating an entirely new framework, government should facilitate industry adoption of globally recognised models, ensuring alignment with international partners. Frameworks such as MITRE's Threat-Informed Defence and Europe's TIBER-EU program already provide robust, intelligence-led approaches. Requiring Australian-only frameworks risks duplication, cost, and misalignment with supply chains.

This plan should therefore focus on contextualising existing global standards for Australian conditions, offering clear guidance on tailoring them to local regulatory and operational environments. Where gaps exist, enhancements can be layered onto international frameworks rather than starting from scratch.

Government's role is to harmonise requirements, reduce regulatory fragmentation, and provide practical guidance on what constitutes "good practice" in Australia. By aligning with global best practice while tailoring to local needs, Australia can uplift industry posture efficiently and remain interoperable with international partners.

Question 26

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

Blocking threats at scale requires shifting from reactive response to proactive prevention, underpinned by intelligence-led collaboration. Today, valuable threat insights often remain siloed, limiting their impact. This plan should position the government as a central aggregator and distributor of anonymised, actionable intelligence, ensuring that patterns of malicious activity can be blocked before reaching consumers and critical infrastructure.

A true "open garden" collaboration between vendors such as ISPs, telcos, and technology vendors are critical. Encouraging software, hardware, and service providers to share security insights, patching strategies, and mitigations in a coordinated manner reduces duplication of effort and ensures that preventive measures reach the widest possible audience. The Government can facilitate joint initiatives that block threats at the network layer, disrupt scam infrastructure, and provide coordinated patching strategies. To maximise reach, these efforts must extend beyond traditional critical infrastructure sectors and include SMBs and NFPs, which often lack the capacity to act independently.

The Government should also invest in shared platforms that translate adversary tactics into practical mitigations. Providing standardised playbooks, automated indicators, and prevention-first guidance allows industry to operationalise intelligence quickly.

Government-led frameworks, workshops, and playbooks can help organisations prioritise mitigations based on the most credible threats, ensuring resources are allocated efficiently to block attacks before they impact consumers, critical infrastructure, or sensitive data.

By combining real-time intelligence sharing, coordinated vendor collaboration, and prevention-first guidance, this plan can enable industry to block threats at scale, reducing systemic cyber risk across all levels of the economy.

Question 27

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

Safe browsing features and deceptive warning pages are proven mechanisms for protecting consumers, but their effectiveness depends on scale, accuracy, and user trust. To reduce harm, government should encourage closer collaboration with browser developers, search engines, social media platforms, and telcos to ensure warnings are timely, prominent, and easy for users to understand.

A prevention-first approach is essential. Social media platforms and web service providers must take a more proactive role in tackling scams, phishing, and fraudulent content by identifying and removing fake accounts and malicious campaigns quickly. Automated detection tools, combined with human review, can significantly reduce exposure before scams reach consumers. At the same time, AI-driven analytics can dynamically assess and flag emerging scam and phishing sites in near real time, with protections extended beyond traditional browsers to mobile devices and IoT platforms, given the growing reliance on these technologies.

Equally critical is intelligence sharing and coordination. Platforms, government agencies, and industry should exchange data on emerging scams, phishing URLs, and adversary tactics through trusted channels, enabling faster takedowns and real-time warnings across multiple digital environments. Integration of threat feeds into browsers, search engines, and social platforms would allow deceptive content to be flagged consistently and accurately.

Technical measures must be complemented by consumer education and awareness. Government-led campaigns — amplified through partnerships with banks, telcos, and ISPs — should explain why warnings appear, encourage consumers to heed them, and promote reporting of suspicious content. Contextual alerts and trusted, relatable messaging will help build user confidence in safe browsing mechanisms.

Finally, coordinated intelligence sharing between government, industry, and platform owners will ensure that malicious sites are identified and flagged quickly. By strengthening both the technical and human dimensions of safe browsing, this plan can reduce consumer exposure to scams and build greater trust in the digital ecosystem.

Question 28

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

Threat sharing ecosystems are most effective when sectors already have baseline maturity, executive sponsorship, and technical capability. In low-maturity sectors such as agriculture,

education, and retail, traditional ISAC models may struggle to deliver value due to limited resources and low participation.

This plan should therefore prioritise building foundational capacity in these sectors before investing in full-scale ISACs. Government-led industry forums, simplified playbooks, and targeted awareness campaigns can raise baseline maturity and readiness. Once capacity improves, ISACs can then be introduced to provide structured, sector-specific sharing.

Barriers such as cost, lack of trust, and privacy concerns must also be addressed. Providing financial incentives, allowing anonymous reporting, and fostering government-backed trust frameworks can encourage participation. Community-driven guidance and baseline standards, supported by the government, to help organisations implement practical cyber controls without requiring complex ISAC infrastructure should also be considered. Finally, there should also be support for threat sharing, as exemplified by the creation of the Health Cyber Sharing Network (HCSN) pilot under Horizon 1 with similar initiatives expanded to other low-maturity sectors.

By focusing first on education, awareness, and simplified collaboration models, this plan can prepare low-maturity sectors for effective threat sharing. Over time, this approach will allow ISACs to thrive where they are most impactful, ensuring investments deliver real resilience outcomes.

Question 29

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

Effective intelligence sharing requires more than compliance—it must deliver timely, actionable insights that organisations can use to prevent harm. This plan should establish a unified national framework for intelligence sharing, aligning cyber threat and scams data under a single coordinated model.

Trusted, sector-specific networks should be expanded to ensure information flows quickly to those who can act. Government can act as a central coordinator, aggregating data from law enforcement, industry, and platforms, and redistributing anonymised intelligence in usable formats.

Operational playbooks must accompany intelligence, translating threat data into practical mitigations for organisations of varying maturity. This is particularly important for SMBs and NFPs, which may lack the expertise to interpret raw threat feeds.

Social media and online platform owners should be required to integrate intelligence into their moderation and scam prevention workflows, ensuring fraudulent activity is disrupted before reaching consumers. Education and awareness campaigns should be

implemented to support industry and end-users through workshops, case studies, and awareness programs that contextualise intelligence and highlight prevention-first practices.

By aligning intelligence sharing under a single coordinated model, supported by practical guidance and platform accountability, this plan can strengthen Australia's ability to disrupt scams and reduce harm at scale.

Question 30

Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?

At present, there is ambiguity around the division of responsibilities between government and industry during a cyber conflict or crisis. While frameworks such as the SOCI Act outline obligations, more clarity is needed to ensure decisive and coordinated responses.

This plan should provide clear guidance on industry's obligations during a conflict or crisis, including thresholds for reporting, expectations for collaboration, and available legal protections. Establishing a Cyber Defence Reserve—calling upon skilled cyber security professionals from industry and academia during national cyber emergencies —would provide surge capability during nationally significant incidents.

Joint cyber exercises must also be scaled. These should simulate realistic adversary campaigns against critical infrastructure, testing not only technical defences but also communication, decision-making, and coordination. Expanding existing programs such as CORIE beyond financial services into other sectors would build national resilience.

Developing a crisis communications plan with clear protocols for crisis scenarios, ensuring timely and accurate sharing between government and the industry as well as pressure-test existing legislative frameworks to identify gaps and barriers for an effective crisis response.

By clarifying roles, establishing surge capacity, and running joint, intelligence-informed exercises, this plan can ensure both government and industry are prepared to act decisively during crises, reducing systemic risk to the nation.

Question 31

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

A strong culture of responsible vulnerability disclosure (VDP) is essential for national resilience, but many organisations hesitate due to legal concerns, reputational risk, and the

resources required to respond. This plan should provide clear incentives and protections to encourage adoption.

First, establishing legal safe harbours for researchers who act in good faith would remove uncertainty and foster trust between the security community and business. Second, government should publish standardised templates and guidelines for VDPs, aligned with international best practice (ISO/IEC 29147 and 30111), reducing the burden on organisations to design frameworks independently.

Incentives such as certification, public recognition, or preferential access to government contracts could reward organisations that adopt effective policies. The Government could also support shared platforms for handling disclosures, providing smaller organisations with the infrastructure to safely manage reports.

By combining legal protections, practical guidance, and reputational incentives, this plan can embed VDPs as a norm across the economy. The outcome will be earlier detection of vulnerabilities, stronger trust with researchers, and reduced systemic risk.

Question 32

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

Yes, there is as whilst mature organisations increasingly adopt their own disclosure programs, many smaller entities lack the capacity to manage them. A national vulnerability disclosure program would fill this gap, creating a trusted, scalable mechanism for safe reporting.

Such a program should act as an intermediary, allowing researchers to submit vulnerabilities centrally, helpful for smaller or less mature businesses who lack the capability to manage disclosures. The Government could then triage, anonymise, and forward reports to affected organisations, ensuring timely remediation. Importantly, legal protections must accompany the program, providing clarity and safe harbour for researchers.

Government should lift maturity across sectors by encouraging high-maturity industries to adopt international standards such as ISO/IEC 29147 and 30111, while providing central disclosure services, awareness, and education to support lower-maturity sectors.

A national program would also enable aggregation of vulnerability data, offering valuable insights into systemic weaknesses across sectors. This intelligence could feed into red-teaming, resilience testing, and targeted policy interventions.

By establishing a central, government-supported mechanism, this plan would both protect researchers and uplift organisations of all maturities. The result would be faster remediation, stronger collaboration, and reduced national exposure to zero-day exploitation

3.4 Shield 4: Protected critical infrastructure

Question 33

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

The *Security of Critical Infrastructure (SOCI) Act* is internationally recognised as a world-leading framework, significantly strengthening baseline security. However, its effectiveness depends on clarity, proportionality, and consistent enforcement. For larger operators, obligations are proportionate, but smaller entities often struggle with compliance due to resource constraints. Some requirements are viewed as complex or duplicative, creating administrative burden.

To improve understanding, government should provide sector-specific guidance and practical implementation tools. Independent audits could validate compliance and build confidence, while financial incentives could support smaller operators in meeting obligations. A regular review process should ensure that SOCI requirements evolve in step with emerging technologies such as AI, IoT, and 6G.

In summary, the SOCI Act provides a strong foundation but requires continual refinement. By tailoring obligations proportionately, simplifying compliance, and ensuring enforcement, this plan can ensure that SOCI continues to protect Australia's most vital assets effectively.

The SOCI Act has significantly uplifted the baseline resilience of Australia's critical infrastructure and is widely regarded as a leading model internationally. However, effectiveness depends on proportionality, clarity, and enforceability. Larger operators generally have the resources to meet obligations, but smaller operators face disproportionate challenges due to cost and complexity.

This plan should address these disparities by tailoring requirements based on risk and sector maturity. Simplified compliance models, practical implementation guidance, and subsidised support would reduce barriers for smaller entities. Independent audits and stronger regulator collaboration can improve enforcement, while regular reviews will ensure the Act keeps pace with evolving threats such as AI and 6G.

Overall, SOCI is effective, but refinement is required to ensure obligations are equitable, outcomes-focused, and consistently applied. By addressing proportionality and maintaining a dynamic review process, this plan can ensure SOCI continues to protect Australia's most critical assets.

Question 34

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

While this plan acknowledges the risks posed by AI, quantum computing, and emerging technologies, current frameworks do not yet prescribe the practical safeguards required to reduce harm. AI systems, for instance, should be subject to mandatory red-teaming against adversarial manipulation prior to deployment in critical sectors such as finance, healthcare and government services, alongside secure MLOps practices and model transparency requirements such as utilizing a Model Software Bill of Materials (SBOM). Similarly, Australia needs a clear national roadmap for post-quantum cryptography adoption, including inventory, prioritisation, and phased migration.

Supply chain risks remain under-addressed, particularly among SMBs and NFPs, which often lack resources to secure interconnected services. Operational technology presents another challenge: long lifecycles and bespoke environments demand tailored security standards and resilience testing.

The growing exploitation of personal data by brokers and AI analysis also raises systemic risks not adequately captured under existing frameworks.

By embedding prevention-first safeguards for emerging technologies, strengthening supply chain resilience, and addressing data exploitation risks, this plan can close current gaps and ensure frameworks remain fit for purpose.

Question 35

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

While stringent regulation is justified given the scale of cyber risk, many stakeholders — particularly SMBs and NFPs — find the current framework complex and burdensome, with requirements like those under the SOCI Act difficult to meet.

The challenge is ensuring compliance costs do not outweigh the intended benefits. To achieve proportionality, government should simplify and harmonise overlapping regulations, provide sector-specific guidance and practical tools, and adopt **a** tiered compliance model where smaller, lower-risk entities face less onerous requirements than larger, high-risk organisations. This balance would maintain strong protections while ensuring obligations remain achievable across all sectors.

Question 36

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

Critical infrastructure operators need sector-specific, practical, and affordable support to strengthen resilience. The Government should set prescriptive baselines informed by adversary behaviours and provide practical playbooks, reference architectures, and independent audits to guide uplift. Access to subsidised cyber ranges, red-team style adversary emulation, and independent assurance labs would allow operators—especially smaller ones—to test and validate defences in realistic conditions.

Financial incentives, such as grants, tax benefits, insurance adjustments, and subsidised vouchers, would encourage investment in resilience, while training programs and awareness initiatives help build a stronger security culture. The national cyber intelligence hub should evolve from only sharing indicators of compromise to curating adversary TTPs and publishing tested mitigation strategies, supported by industry ISACs.

Coordinated exercises across sectors will ensure operators are prepared for cross-domain incidents.

In short, government's role is to provide clarity, shared infrastructure, and incentives, while operators take responsibility for embedding resilience. By working together, this plan can uplift critical infrastructure maturity, ensuring continuity of essential services under growing threat. Critical infrastructure operators need sector-specific, practical, and affordable support to strengthen resilience. This plan should provide prescriptive baselines informed by adversary behaviours, alongside reference architectures, validated playbooks, and configuration guides to help operators implement controls effectively.

Government-funded cyber ranges and model red-team environments would allow operators to test defences under realistic conditions. Independent audits, subsidised through vouchers for smaller operators, could help validate controls and identify gaps. Financial incentives—including grants, tax offsets, and insurance benefits—would further encourage proactive investment in resilience.

The government should also expand national intelligence-sharing hubs, shifting from indicator feeds to curated adversary behaviours and tested mitigation strategies. This ensures operators have access to actionable insights, not just raw data.

In summary, government's role is to provide clarity, shared infrastructure, and incentives, while operators take responsibility for embedding resilience. By combining guidance, tools, and incentives, this plan can uplift maturity across critical infrastructure, ensuring continuity of essential services even under sustained cyber pressure.

Question 37

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

Private sector partners often struggle with fragmented, overlapping, and complex requirements. This plan should focus on harmonisation, clarity, and practical support. Aligning certifications and technical controls across frameworks such as IRAP, Essential Eight, SOCI, and ISO would reduce duplication and build confidence that investments deliver outcomes recognised across multiple programs.

The Government can also provide practical implementation tools—reference architectures, configuration baselines, and prevention-first playbooks—that translate obligations into tested technical patterns. Shared assurance services, such as subsidised cyber ranges and independent labs, would allow vendors and operators to validate controls against government-defined threats before certification.

Procurement levers can be used to reward companies that demonstrate validated resilience, while recognition programs build reputational value for early adopters. Two-way engagement is essential: ISCAs and advisory boards should be enhanced and trusted forums should allow private sector partners to provide feedback on where requirements create friction or gaps, ensuring continuous refinement.

By simplifying, harmonising, and incentivising requirements, this plan can ensure security obligations are seen not as burdens but as enablers of stronger, more consistent resilience across the economy.

Question 38

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

Government frameworks such as the *Essential Eight* and the SOCI Act are increasingly influential in shaping private sector practices. The Essential Eight is widely recognised as a baseline, particularly in boardrooms, but is often misunderstood as a complete framework rather than a tactical control set. To be effective, it must be integrated into broader governance and risk management approaches.

Private sector adoption is also hindered by complexity and overlap between different frameworks, which can create unnecessary compliance costs. Larger organisations are better positioned to align with multiple standards, while SMBs and NFPs often find the burden disproportionate.

There is also growing recognition that compliance does not equal prevention. Meeting a checklist may satisfy regulatory obligations, but it does not guarantee resilience against real adversaries. To mature, organisations need to adopt a threat-informed, prevention-first mindset — where government baselines like the Essential Eight are integrated into broader governance frameworks, continuously validated through testing, and mapped against current adversary behaviours.

Overall, Government requirements are shaping private sector practices — but clearer guidance on how technical baselines should connect to governance and threat-informed defence would help prevent misapplication and give boards more confidence that compliance translates to genuine resilience.

3.5 Shield 5: Sovereign capabilities

Question 39

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

A sustainable, skilled cyber workforce is fundamental to national resilience. The Government's role should be to convene, fund, and enable programs that accelerate growth without creating unnecessary complexity. This plan should prioritise practical pathways, shared infrastructure, and diversity.

Apprenticeships, micro-credentials, and work-integrated learning programs can provide immediate, hands-on experience for students and career changers. Shared cyber ranges and adversary-emulation labs, co-funded by government, would scale training capacity across industry and education providers. Endorsing globally recognised frameworks such as NICE/NIST or SFIA, and mapping them to Australian requirements, would standardise skills development and prevent duplication.

Australia's cyber workforce can be strengthened by expanding programs like the Cyber Workforce Playbook, supporting mid-career transitions, and promoting STEM education and early engagement for underrepresented groups, including First Nations people. Establishing a national certification framework will also standardize skills and qualifications, ensuring a consistent and trusted talent pipeline.

Retention incentives, including grants or tax benefits for employers supporting reskilling and mobility, can help sustain the workforce. Diversity initiatives, such as scholarships for underrepresented groups, will broaden participation and ensure different perspectives strengthen national capability. Promote a threat-informed mindset by ensuring training and pilot programs are anchored in adversary behaviours and prevention-first control validation, not compliance checklists. This ensures the workforce is prepared to deliver resilience, not just paperwork.

By focusing on shared infrastructure, practical pathways, and diversity, this plan can accelerate workforce growth while ensuring skills are relevant, threat-informed, and future-ready.

Question 40

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

Successful initiatives in Australia and abroad show that mid-career transition programs work best when they provide practical, supported pathways. The *Cyber Workforce Playbook* and inaugural *Cyber Workforce Summit* have provided valuable direction domestically, while industry-led bootcamps and reskilling programs overseas have demonstrated how professionals from finance, defence, and education can pivot into cyber roles.

Diversity-focused STEM programs, such as scholarships and mentoring initiatives, have also proven effective in increasing participation by women, First Nations people, and culturally diverse communities. By combining financial support with mentorship and networking, these initiatives address both skills gaps and systemic barriers to entry.

This plan should expand national mid-career transition programs, particularly those offering short, intensive reskilling modules mapped to recognised skill frameworks. Scaling mentorship and sponsorship programs would further strengthen support for underrepresented groups.

By investing in these proven models, Australia can not only close workforce gaps more quickly but also build a cyber workforce that reflects and protects the diversity of the nation.

Question 41

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

Several industries hold skills highly transferrable to cyber. Professionals in defence and intelligence bring expertise in risk management and threat analysis. Finance and audit specialists contribute capabilities in compliance, data security, and fraud detection. Healthcare workers have experience in safeguarding sensitive data and operating under strict regulatory conditions, while educators possess strong communication and training skills, valuable for awareness and incident coordination roles.

Existing research, such as the NIST NICE framework and the AISA Cyber Skills Survey, provides structured ways to map these skills into cyber roles. These studies confirm the potential of lateral entry pathways, particularly when paired with targeted micro-credentials and work-integrated learning.

This plan should formalise recognition of transferable skills, fund rapid training pathways, and support campaigns to raise awareness of cyber career opportunities for professionals in

adjacent industries. By leveraging existing talent pools, Australia can scale its cyber workforce more quickly and sustainably.

Question 42

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

Research priorities must be anchored in real-world adversary behaviours and aligned with national resilience goals. Today, too much effort is placed on static indicators of compromise, which struggle to keep pace with adaptive threats. This plan should foster collaboration between industry, academia, think tanks and government through coordinated research agendas that are threat-informed and operationally relevant.

Government can set clear national themes, such as AI-enabled adversary modelling, quantum-resistant encryption, and continuous resilience testing. Collaborative centres of excellence should bring together academic expertise, industry telemetry, and government intelligence to co-develop solutions. Funding should prioritise projects that translate directly into operational outcomes, such as behaviour-based detection, automated prevention controls, and adversary-emulation environments.

Think tanks can provide independent policy analysis, ensuring that technical innovation aligns with regulatory and ethical expectations. Shared cyber ranges and digital twins of critical infrastructure should serve as testbeds for research translation, enabling innovation to be validated before deployment.

A national research agenda co-developed by government, industry, and academia should prioritise strategic areas such as AI, quantum computing, and data security, supported by multidisciplinary research hubs to address complex cyber security challenges. To maximise impact, platforms for sharing research findings and best practices across sectors are essential.

By aligning research priorities to adversary behaviours, co-funding applied innovation, and fostering multi-sector collaboration, this plan can ensure that cyber research delivers measurable outcomes for Australia’s strategic, economic, and community resilience.

Question 43

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

A stronger partnership between government and academia requires long-term engagement structures, not ad hoc projects. This plan should prioritise durable funding models, shared research infrastructure, and structured exchange programs.

Long-term funding agreements for collaborative projects would provide certainty for universities and ensure research aligns with national priorities. Exchange programs between policymakers and academics could deepen mutual understanding, while joint conferences and workshops would provide regular forums for collaboration. Hackathons and innovation challenges, co-hosted by universities and agencies, could further stimulate applied research in areas such as AI resilience and quantum security.

For students, fellowships and internships in government cyber units would create early exposure to policy environments, while secondments of government staff into universities would help embed practical, operational insights into curricula.

By building stronger institutional and personal relationships, this plan can bridge the gap between research and policy, fostering a culture of collaborative culture.

Question 44

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

Australia cannot, and need not, develop every cyber capability domestically. Sovereignty should be prioritised in areas critical to national security, resilience, and economic continuity. This plan should therefore begin with a comprehensive audit of existing domestic capabilities, combined with a risk-based assessment of gaps that could expose Australia to undue dependence or systemic risk.

Priority should be given to capabilities that directly protect critical infrastructure and sensitive government systems, such as advanced detection, incident response, and secure data storage. Intelligence aggregation, adversary modelling, and red-teaming capabilities are also strategic priorities, as they underpin decision-making and national resilience.

Where gaps exist in less critical areas, partnerships with trusted allies should be pursued, leveraging global expertise while ensuring domestic delivery. AUKUS-style collaboration models can provide a pathway for shared development that strengthens both sovereignty and alliances.

By identifying critical functions, prioritising high-risk gaps, and leveraging trusted partnerships where appropriate, this plan can ensure sovereign capabilities are focused, sustainable, and strategically aligned.

Question 45

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

Concentration risk arise when too much reliance is placed on a small number of ICT providers, particularly cloud platforms and telecommunications networks. This can create systemic vulnerabilities if those providers experience compromise, outage, or misaligned incentives. It can also limit innovation by reducing opportunities for specialist vendors.

Mitigation requires a balanced approach. Transparency and independent assessment of platform providers' security controls should be mandated, ensuring accountability. Standards promoting interoperability would make it easier for organisations to diversify suppliers without prohibitive switching costs. Government procurement policies can encourage vendor diversity, supporting local providers and startups.

Additionally, developing contingency plans—such as backup hosting arrangements or multi-cloud strategies—can reduce exposure to single points of failure. Regulators should also monitor concentration risk at a sectoral level, ensuring that resilience is considered not just by individual organisations but across the ecosystem.

By combining transparency, interoperability, and vendor diversity, this plan can mitigate ICT concentration risk while maintaining the benefits of scale and innovation from global providers.

3.6 Shield 6: Strong region and global leadership

Question 46

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

Attributions, advisories, and sanctions are important signaling tools, but their deterrent effect is limited, particularly against non-state actors such as ransomware groups. Advisories and attribution should therefore become more frequent, detailed, and technically actionable, providing defenders with behaviour-based guidance while still protecting sensitive intelligence.

To strengthen deterrence, this plan should also adopt forward-leaning disruption measures. These include regional cooperation to dismantle scam centres, financial disruption of illicit flows, and coordinated takedowns of malicious infrastructure. Enhancing operational collaboration with allies can amplify these efforts, ensuring adversaries face higher costs and reduced safe havens.

Australia should also invest in building coalitions for coordinated sanctions against state-sponsored actors, reinforcing diplomatic pressure. At the same time, capacity-building support for regional partners can reduce vulnerabilities that adversaries exploit.

By combining attributions, advisories, and sanctions with proactive disruption, financial measures, and regional coalition-building, this plan can move Australia from reactive response to proactive deterrence in cyberspace.

Question 47

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

Regional engagement is essential, as many threats affecting Australia originate in or transit through Southeast Asia and the Pacific. Expanding the SEA-Pacific Cyber program should strengthen partnerships by combining capacity building, intelligence sharing, and diplomatic engagement.

Technical assistance programs can help regional partners uplift cyber maturity, particularly in critical infrastructure, law enforcement, and digital governance. Australia should provide training, incident response support, and shared playbooks to ensure partners can detect and respond to threats effectively. Joint cyber exercises—covering tactical, operational, and strategic levels—would build collective preparedness.

Diplomatically, Australia must continue to address large-scale scam centres in the region, which not only defraud Australians but also involve human rights abuses such as forced labour. Coordinated law enforcement operations, combined with regulatory interventions, can help dismantle these networks.

Finally, fostering regional intelligence exchanges and harmonised standards will enhance interoperability. By combining capability development with strong diplomatic pressure and shared intelligence, this plan can build a safer, more resilient cyber ecosystem across Southeast Asia and the Pacific.

Question 48

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

Yes. Cyber RAPID has strong potential to evolve from an incident-response model into a proactive resilience hub for both Australia and its regional partners. This plan should expand its scope to include anonymised lessons learned from incidents, adversary playbooks, and assessments of effective controls—mirroring the aviation safety model, where failures are analysed globally to prevent recurrence and include proactive threat hunting and intelligence sharing.

Regionally, Cyber RAPID could extend support by sharing threat intelligence and validated mitigation strategies with Southeast Asian and Pacific partners. Joint investigations, capacity-building initiatives, and regional exercises could be coordinated through Cyber RAPID, allowing partners to learn from Australia's experiences with advanced adversaries.

With additional funding and mandate, Cyber RAPID could also develop a regional threat-blocking framework, coordinating with telcos and ISPs to disrupt malicious infrastructure across borders. By evolving into a proactive, intelligence-sharing and resilience-building entity, this plan can ensure Cyber RAPID delivers greater value both domestically and regionally.

Question 49

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

Australia should focus its international engagement on forums that shape norms in practical and enforceable ways. The *Geneva Dialogue on Responsible Behaviour in Cyberspace* offers an important platform to operationalise UN cyber norms, with multi-stakeholder participation from governments, industry, and academia. Active participation here would

allow Australia to shape global approaches to supply chain security, critical infrastructure protection, and responsible vulnerability disclosure.

Regional forums such as ASEAN are equally important, particularly for capacity building and alignment on cybercrime disruption. Participation in technical bodies such as the ITU and standards organisations (ETSI, ISO, NIST collaborations) will ensure Australia's interests are embedded in emerging technology standards, including AI and quantum security.

Finally, engaging through the World Economic Forum and other multilateral venues can amplify Australia's role as a trusted, values-driven leader. By prioritising forums that combine technical, diplomatic, and operational relevance, this plan can ensure Australia helps shape global rules and norms in ways that advance national interests and regional stability.

Question 50

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

Regulatory alignment is critical for interoperability, trade, and resilience. This plan should prioritise alignment with global standards in three areas: emerging technology, data protection, and critical infrastructure.

For emerging technologies, Australia should align with frameworks shaping AI security and quantum readiness, ensuring that global supply chains remain interoperable. For data protection, alignment with the EU's *GDPR* and similar privacy regimes would provide consistency and facilitate cross-border cooperation.

Incident reporting requirements should also be harmonised internationally, reducing complexity for multinational organisations and improving global intelligence sharing. Alignment with initiatives such as Europe's *NIS2 Directive* and Singapore's *Cybersecurity Act* would strengthen resilience of critical sectors while supporting regional partnerships.

By prioritising interoperability, consistent standards, and harmonised reporting, this plan can ensure Australian organisations are not disadvantaged globally, while embedding resilience into international collaboration.