# Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

The ISC2 Sydney Chapter is a not-for-profit professional association dedicated to advancing the information security field in Australia. As an approved chapter of ISC2, it operates under a mission encapsulated by the acronym SAGE: Support an open platform for sharing cybersecurity experiences, actively mentor newcomers, give back to the community by aiding non-profits, and Endeavour to boost public cyber awareness, especially among seniors and children. Governed by a structured board and detailed bylaws, the chapter promotes collaboration, ethical practice, and continuous professional development. It offers tiered membership Professional, General, and Student each with distinct rights and responsibilities, fostering an inclusive environment for cybersecurity professionals to contribute to national cyber resilience and community safety.

*ISC2 SYDNEY CHAPTER INCORPORATED*
*Registration Number # INC2500857*
*Email address:* [redacted]

## Executive Summary

This submission by the ISC2 Sydney Chapter responds to the Horizon 2 consultation, emphasizing the need for standardized frameworks, enhanced public-private collaboration, and inclusive cyber uplift programs. Key recommendations include adopting NIST CSF for consistent cyber maturity measurement, establishing a national ISAC for real-time threat intelligence sharing, and implementing tailored support for SMEs and NFPs through simplified standards and financial incentives. The chapter also advocates for stronger regional engagement, proactive ransomware defences, and workforce development initiatives to address skill shortages. These measures aim to build a resilient, collaborative, and forward-looking cybersecurity ecosystem aligned with Australia's strategic goals.

## Summary of the paper

The ISC2 Sydney Chapter recommends adopting the NIST Cybersecurity Framework as a national standard to harmonize diverse regulatory requirements and reduce compliance overhead. It proposes the creation of an Australian Information Sharing and Analysis Centre (A-ISAC) to facilitate real-time threat intelligence exchange across government and industry sectors. For SMEs and NFPs, the chapter suggests simplified, sector-specific versions of international standards, supported by financial incentives such as tax breaks and cyber hygiene vouchers. Additional measures include expanding ransomware playbooks into high-risk sectors, implementing IoT security labelling based on ETSI EN 303 645, and fostering regional cyber resilience through joint exercises and capacity-building programs. These recommendations aim to close maturity gaps, enhance collective defence, and ensure Australia's cyber strategy remains adaptive and inclusive.

ISC2 CHAPTER SYDNEY

## Recommendations:

| | |
|---|---|
| **2.1.1** | **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?** |

**Artificial Intelligence (AI) Governance:**
AI introduces both opportunities and risks, from detecting threats faster to enabling deepfakes and supply chain manipulation. Establishing a national AI governance framework ensures ethical adoption, safeguards against malicious misuse, and supports industries managing sensitive citizen data.

**Quantum Readiness:**
Future quantum computers will be capable of breaking today's encryption. Expanding post-quantum cryptography transition planning through sector-specific roadmaps and public–private collaboration will ensure resilience against adversaries already storing encrypted data for later decryption.

**Cloud and Edge Infrastructure Security:**
The growing reliance on cloud and edge ecosystems demands consistent national guidance. Publishing security standards and running awareness campaigns will close capability gaps across small business and critical sectors, ensuring scalable protections across Australia's digital economy.

**Blockchain for Digital Identity:**
Blockchain identity systems hold promise but carry risks. Regulatory sandboxes and pilot programs will help validate secure use cases, balancing innovation with safeguards for sensitive citizen information.

The recommendations are critical as Australia shifts toward AI-driven, cloud-based, and blockchain-integrated systems while facing quantum disruption. AI governance protects against disinformation and exploitation. Quantum readiness ensures long-term cryptographic integrity. Cloud and edge guidance address systemic gaps identified in Horizon 1, strengthening SME and enterprise defences. Blockchain pilots allow government to shape secure adoption rather than react to poorly governed rollouts. Together, these measures support a resilient national posture, aligned with international standards and adaptive to rapid innovation. Skilled migration and workforce programs must complement this strategy to resolve talent shortages, ensuring Australia develops local expertise while securing its place in the global cyber economy.

| | |
|---|---|
| **2.2.2** | Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government? |

**Cyber Wardens for SMEs:**
Queensland's partnership with COSBOA on the Cyber Wardens Program equips small business staff with practical, industry-specific cyber skills. Expanding this nationally would uplift SME resilience, creating a consistent standard for frontline cyber hygiene across all states.

**Centralised Threat Reporting & Intelligence:**
NSW's Cyber Security Portal simplifies incident reporting and intelligence sharing across agencies. Scaling this to a national level would enable faster, coordinated responses, reduce duplication, and serve as a foundation for whole-of-government cyber collaboration.

**Vulnerability Disclosure & Research Collaboration:**
WA's Cyber Disclosure Program provides a trusted channel for ethical hackers to report vulnerabilities. Replicating this model would build trust, fix weaknesses proactively, and embed responsible reporting across all levels of government.

**Cyber Skills Pathways for Vocational and Government Cybersecurity Workforces:**
ACT's Certificate IV in Cyber Security and SA's workforce upskilling initiatives directly address talent shortages. Expanding such programs nationally would standardise vocational pathways, strengthen pipelines into the workforce, and support long-term resilience.
For government workforce, Queensland government is running Entry-level Cyber Training to upskill public servants and council staff with IT or cyber-related responsibilities. This includes bridging programs leading to Certificate IV in Cyber Security. These programs can be expanded nationally to standardise government workforce cyber security skill level and bridging with the industry standard.

Expanding these state-led initiatives nationally ensures Australia benefits from proven models while reducing fragmentation across jurisdictions. Cyber Wardens uplift SMEs, a major attack vector often overlooked. NSW's portal demonstrates how coordinated intelligence sharing reduces response times. WA's disclosure program builds public trust and taps into a motivated research community to secure systems before adversaries strike. ACT and SA highlight the importance of tackling workforce shortages through vocational pathways and government-led skills exercises, which align with Horizon 2's focus on talent development. Together, these replicated initiatives would enable a harmonised national framework where states provide leadership, territories support local engagement, and the federal level ensures alignment with national objectives. This approach minimises duplication, strengthens systemic resilience, and creates an adaptive, inclusive, and whole-of-nation cyber uplift.

| 2.3.3 | Does the high-level Model resonate and do you have any suggestions for its refinement? |
|---|---|

**Adopt NIST CSF as a Core Framework:**
The NIST Cybersecurity Framework provides a holistic structure covering governance, identification, protection, detection, response, and recovery. Its tiered maturity levels make it scalable for small and large organisations, enabling a harmonised and internationally recognised improvement path.

**Standardise Terminology through a National Glossary:**
Aligning with the NIST Cybersecurity Glossary or creating an Australian national glossary would reduce ambiguity, enable consistent communication, and ensure interoperability across sectors. Clear terms improve coordination, incident handling, and cyber maturity assessment.

**Create a Master Reference Model with Crosswalks:**
Mapping CPS 234, SOCI, ISM, ASD Essential 8, and state frameworks (e.g., NSW CSP) into a unified model would reduce duplication, clarify overlaps, and help organisations see how compliance fits within a bigger national picture.

The current high-level model is a strong foundation, but refinement is needed to minimise fragmentation and complexity identified in Horizon 1. NIST CSF adoption ensures harmonisation with global practices while complementing Australia's Essential 8 technical controls. The use of a national glossary improves clarity across government, industry, and international partners. Developing a master reference model with crosswalks aligns regulatory obligations across sectors, helping organisations reduce compliance overhead and focus on genuine resilience uplift. Incorporating maturity levels (from NIST CSF tiers or SMB1001) offers a progressive pathway that enables smaller organisations to start with self-assessment while larger ones pursue higher certifications. Collectively, these refinements make the model scalable, interoperable, and future-proof, supporting Horizon 2's goal of consistent national cyber uplift.

| | |
|---|---|
| **2.3.4** | Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes? |

**Centralised Portal with Standardised Metrics:**
A national portal should serve as the hub for structured data submission, featuring standardised metrics such as a transparent "cyber health score." This scorecard would provide businesses with a simple benchmark to track resilience progress over time.

**Multi-Channel Feedback System:**
Combining structured surveys, sector-specific roundtables, and NFP cyber community engagement would capture diverse perspectives. This ensures both large enterprises and underserved groups such as SMEs and councils are represented in national situational awareness.

**Dynamic Feedback Loops for Policy Adaptation:**
The system must enable continuous learning. Real-time data from attacks, threat trends, and sector performance should trigger rapid review and adjustment of policies, awareness programs, and funding priorities, rather than waiting for periodic evaluations.

**Clear Accountability and Role Mapping:**
A matrix assigning responsibility across federal, state, territory, and private sectors would enable progress tracking and ensure no key area is overlooked. Defined accountability strengthens ownership and improves transparency of outcomes.

Monitoring effectiveness requires more than one-way data collection,it must integrate real-time feedback, actionable metrics, and clear accountability. A centralised portal with standardised metrics like cyber health scores would make outcomes measurable and transparent. Structured roundtables and surveys would capture ground-level realities, particularly from SMEs and regional communities. Continuous monitoring services (e.g., SecurityScorecard-style tools) could complement this by providing external benchmarks. A dynamic feedback loop ensures that policy evolves with the threat landscape, closing gaps faster. Finally, clarifying roles across all levels of government and industry ensures that progress is not only tracked but also attributable. Together, this approach supports continuous improvement, transparency, and adaptive resilience in Horizon 2.

| 3.1.5 | What could government to do better target and consolidate its cyber awareness message? |
|---|---|

**Standardise and Simplify Language:**
Adopt globally recognised frameworks such as the NIST Cybersecurity Glossary or create an Australian national glossary. Consistent terminology reduces confusion, especially for SMEs and vulnerable groups, making guidance clearer, trusted, and easier to adopt.

**Embed Cyber Safety in Everyday Channels:**
Rather than relying only on standalone campaigns, cyber reminders should be integrated into communications people already use, rates notices, tax letters, utility bills, and digital service platforms (e.g., MyGov, Medicare, Service NSW). This normalises awareness and reaches wider audiences.

**Unify Messaging Under a National Brand:**
A single trusted cyber brand (building on Act Now, Stay Secure) would reduce fragmentation across federal and state initiatives. Clear, centralised branding ensures credibility, increases visibility, and strengthens the public's confidence in cyber safety guidance.

**Timely and Contextual Messaging:**
Awareness efforts should be tailored and relevant, surfacing scam alerts during high-risk periods (e.g., tax time) or prompting phishing awareness during login to digital platforms. This increases impact by connecting advice to real-world actions.

Horizon 1 highlighted that fragmented and inconsistent language reduced the effectiveness of cyber awareness campaigns, particularly for non-technical users. Standardising terminology and unifying messaging would streamline communication, foster trust, and ensure advice is acted upon. Embedding cyber reminders into everyday channels leverages existing touchpoints to reach groups often overlooked by digital-first campaigns, such as the elderly and small business operators. Timely, contextual prompts increase the relevance of cyber safety information, driving behavioural change rather than passive awareness. Consolidating efforts under a single national brand ensures consistency, visibility, and authority, transforming cyber awareness from occasional campaigns into a practical, daily reinforcement of secure habits.

| | |
|---|---|
| **3.1.6** | 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? |

**Cyber Wardens Program:**
Delivered under Horizon 1, Cyber Wardens successfully engaged non-technical SME staff by simplifying cyber awareness and budgeting. Expanding it with sector-specific modules and expert-led training would help SMEs move beyond basic hygiene toward deeper resilience.

**Essential Eight (ACSC):**
The Essential Eight framework has provided clear, practical controls for organisations. Its uptake could be scaled further through tailored education packages, vocational courses, and integration into workforce training, ensuring consistent adoption across industries and government.

**Hands-On Skill Development (CTFs & Bug Bounties):**
Government-sponsored "Capture the Flag" competitions and Bug Bounty programs, run with security associations, offer practical exposure for students and early-career professionals. These encourage problem-solving, real-world learning, and build pathways into the cyber workforce.

**Integration into Education and Vocational Pathways:**
Embedding standardised terminology and cyber modules in schools, TAFE, and higher education will normalise cyber literacy from an early stage. Nationally aligned curricula can ensure consistent capability building across diverse regions and learner groups.

Programs like Cyber Wardens and Essential Eight have shown success by using plain language, practical controls, and engagement tailored to SMEs. However, their non-technical focus leaves a gap that could be addressed by partnerships with cyber communities to provide technical depth. Scaling up CTFs and bug bounty initiatives adds hands-on, skill-building experiences that excite younger learners and foster talent pipelines. Embedding cyber awareness into formal education and vocational pathways ensures consistency and longevity, equipping future workers with a baseline of cyber skills regardless of industry. Together, these initiatives create a layered approach: grassroots awareness for SMEs, structured resilience frameworks for organisations, and skill pipelines for the future workforce, aligning awareness with capability uplift.

| | |
|---|---|
| **3.1.7** | How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)? |

**Embed Cyber Resources into Everyday Platforms:**
Integrate services like Cyber Wardens or ACNC guidance into familiar platforms (e.g., MyGov, ATO portals, business banking apps). Using an opt-out model reduces friction, ensuring SMBs and NFPs receive guidance without extra effort.

**Make Guidance Simple and Relevant:**
Use plain language that connects cyber risks to business outcomes,lost revenue, fines, or reputational harm. Provide checklists, short videos, and real-world testimonials from peers to make guidance relatable, practical, and less overwhelming.

**Create a National Vendor Catalogue:**
Develop a government-backed marketplace of pre-approved, discounted security solutions (MFA, EDR, secure email). This simplifies procurement, reduces cost barriers, and ensures SMBs/NFPs adopt trusted, baseline protections without navigating vendor complexity.

**Leverage Trusted Advisors & Local Networks:**
Equip accountants, lawyers, and industry associations with cyber advice so they can deliver it during existing interactions. Partnering with chambers of commerce and local NFP hubs ensures broader reach and contextualised support.

**Incentivise and Recognise Adoption:**
Introduce subsidies, tax rebates, cyber insurance discounts, and training vouchers for participants. Publicly recognise “cyber smart” SMBs and NFPs through awards and case studies, creating visible role models and encouraging wider uptake.

Horizon 1 revealed that while resources exist, uptake is limited by complexity, cost, and lack of relevance. Embedding resources in familiar platforms ensures exposure; simplifying advice drives comprehension; and a national vendor catalogue reduces procurement challenges. Partnering with trusted advisors leverages existing relationships to build credibility. Incentives and recognition create clear value propositions, addressing time and resource constraints. Together, these measures move cyber awareness from optional to practical and rewarding, boosting adoption across SMBs and NFPs while strengthening Australia’s collective resilience.

| | |
|---|---|
| **3.1.8** | 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? |

**Unify and Simplify Cybersecurity Guidance:**
Government and industry should co-develop a single, plain-language baseline standard aligned with NIST/ISO and the Essential Eight, but simplified for SMB/NFP contexts. Using co-branded, sector-specific guidance avoids conflicting messages and ensures clarity.

**Build Community-Driven Support Hubs:**
Regional cyber hubs, co-funded by government and industry, can deliver free toolkits, drop-in mentoring, and "cyber wardens" tailored to local sectors (e.g. aged care, charities). Local associations and chambers of commerce can co-host awareness sessions.

**Incentivise Participation and Compliance:**
Introduce tax rebates, training vouchers, grants, and cyber insurance discounts for SMBs/NFPs meeting baseline controls. Industry can integrate cyber checks into procurement and supply chain requirements, creating both carrot and stick incentives.

**Leverage Trusted Networks and Case Studies:**
Equip accountants, business bankers, and NFP advisors with cyber resources so they deliver advice in everyday interactions. Showcase relatable case studies of peers who reduced risk or avoided loss through cyber readiness.

SMEs and NFPs face limited time, funds, and expertise. A fragmented approach risks confusion and low engagement. Simplified, sector-specific guidance co-designed with industry associations addresses real operational needs while maintaining national consistency. Regional hubs provide accessible, localised help, building long-term capacity. Incentives offset cost barriers and drive measurable adoption, while embedding cyber into procurement ensures resilience flows through supply chains. Real-life examples and delivery via trusted advisors enhance credibility and uptake. Together, this integrated, community-led approach creates sustained behavioural change and strengthens Australia's collective cyber resilience.

| | |
|---|---|
| **3.1.9** | What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's? |

**Adapt Global Frameworks into Simplified Versions:**
Standards such as NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and the ACSC Essential Eight provide strong baselines but are often too complex for SMBs and NFPs. These should be simplified into plain-language, sector-specific guidance co-designed with community input to ensure practicality and relevance.

**Leverage Emerging SMB-Focused Standards:**
Developing approaches such as NIST's Small Business Cybersecurity Corner and Australia's Small Business Cyber Resilience Service show how large frameworks can be translated into accessible roadmaps. New efforts like the ISO/IEC 27001 "lite" models and SMB1001 also provide a pathway for resource-limited organisations.

**Use Independent and Flexible Validation:**
To avoid conflicts of interest, self-attestation should be complemented with independent validation via accredited assessors or sector-based auditors. A hybrid model, self-assessment for lower-risk entities and external audit for higher-risk ones, keeps assurance scalable and fair.

**Align with Incentives and Programs:**
Standards adoption should be integrated into existing initiatives like Cyber Wardens and regional cyber hubs, with incentives such as certification subsidies, grants, or cyber insurance discounts. This lowers barriers and embeds standards into practical support mechanisms.

Global standards like NIST CSF and ISO 27001 set rigorous expectations, but without simplification, they remain inaccessible to smaller organisations. By adapting these into tailored, easy-to-use guidance, validated by independent oversight, SMBs and NFPs can adopt security controls proportionate to their risk. Incentivisation ensures uptake, while embedding standards into familiar programs and trusted networks builds sustained engagement. This approach balances international alignment with local practicality, lifting collective resilience without overwhelming smaller players.

| | |
|---|---|
| **3.1.10** | 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? |

**Unique Challenges for NFPs:**
Limited Budgets and Resources: Many NFPs operate on tight funding, restricting investment in IT security, software, and dedicated staff.

**Volunteer Reliance:**
Operations often depend on volunteers with limited technical skills, increasing susceptibility to phishing and misconfiguration.

**Sensitive Data Handling:**
NFPs frequently manage personal, health, or donor information, making them high-value targets for ransomware, fraud, or identity theft.

**Decentralised Structures:**
Federated or multi-branch operations can lead to inconsistent security policies and uneven adoption of best practices.

**Low Awareness and Technical Expertise:**
Staff and volunteers may lack cybersecurity awareness or training, increasing human error risks.

**Government Interventions for Maximum Impact:**
Tailored No-Cost Toolkits: Provide NFP-specific, practical guides aligned with NIST/ISO standards to implement baseline controls.

**Grants and Funding for Cyber Coordinators:**
Support dedicated cybersecurity roles or coordinators in larger NFPs to lead awareness and compliance efforts.

**Volunteer Mentor Programs:**
Partner with local tech communities to deliver mentorship, hands-on guidance, and training for staff and volunteers.

**Tax Incentives and Subsidies:**
Reward NFPs achieving certification or implementing essential controls, lowering financial barriers.

**Simplified Reporting and Compliance Portals:**
Streamline incident reporting and guidance to make it accessible for organisations with limited IT capacity.

NFPs are often resource-constrained yet handle sensitive data that makes them attractive targets. Unlike commercial businesses, they cannot easily invest in cybersecurity or hire specialist staff. Targeted government interventions, practical toolkits, mentorship, funding, and incentives, address

these structural limitations directly. Simplified portals and aligned reporting reduce complexity, while federated mentorship and coordinators ensure consistent practices across branches. By focusing on practicality, accessibility, and affordability, these measures lift cyber maturity in the NFP sector, protecting vulnerable populations, sensitive data, and the broader national digital ecosystem.

| | |
|---|---|
| **3.1.11** | 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? |

**Affordability and Accessibility Challenges:**
Cyber insurance remains largely inaccessible to SMEs and NFPs due to high premiums, complex policy terms, and inconsistent underwriting. Many small organisations also underestimate their cyber risk, viewing insurance as optional rather than essential, while rising global threats drive cost increases and coverage exclusions.

**Simplified Underwriting and Standards:**
Aligning insurance requirements with practical, baseline cybersecurity controls, such as ACSC Essential Eight or NIST CSF, would standardise risk assessments. Simplified policies reduce administrative complexity, making it easier for small entities to meet coverage criteria without specialist expertise.

**Incentives and Public-Private Risk Sharing:**
Government could implement premium subsidies or grants for SMEs/NFPs that adopt baseline controls. Additionally, a public-private cyber insurance pool could spread risk, lowering costs and improving affordability while maintaining market sustainability.

Current cyber insurance uptake among small entities is low, approximately 20% in Australia, primarily due to cost, perceived irrelevance, and complex terms. Standardised, simplified requirements paired with financial incentives and risk-sharing mechanisms directly address these barriers. This approach not only increases accessibility but encourages implementation of essential cybersecurity practices, improving resilience and reducing overall national exposure to cyber threats.

| | |
|---|---|
| **3.1.12** | How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing? |

**Understanding the Threat:**
Ransomware is increasingly targeted at individuals, SMBs, and NFPs, often through phishing, weak credentials, or unpatched systems. Small entities face "big game hunting" attacks, where cybercriminals deliberately target organisations with valuable data or critical services despite limited resources.

**Evolving Threat Landscape:**
The threat is rapidly evolving with AI-driven techniques, enabling more convincing social engineering, automated vulnerability scanning, and tailored attack campaigns. Attackers increasingly exploit cloud and IoT weaknesses, while ransomware-as-a-service models lower technical barriers for criminals.

**Government Interventions:**

**Real-Time Threat Alerts:** Expand alerts through platforms like the Small Business Cyber Resilience Service, providing actionable, timely guidance for SMEs and NFPs.

**Mandatory Cyber Hygiene:** Require multi-factor authentication, regular backups, and ransomware recovery plans for organisations handling sensitive data.

**AI-Powered Simulation Exercises:** Pilot simulations for high-risk sectors to stress-test defences, train staff, and evaluate incident response readiness.

Ransomware has moved from opportunistic attacks to strategically targeted campaigns, particularly affecting smaller entities that often lack dedicated security teams. Real-time alerts increase awareness and rapid response capability, mandatory hygiene establishes a minimum resilience baseline, and AI-driven simulations prepare organisations for emerging attack methods. Collectively, these measures help reduce impact, improve recovery times, and enhance national cyber resilience.

| | |
|---|---|
| **3.1.13** | How could the government further support businesses and individuals to protect themselves from ransomware attacks? |

**Sector-Specific Playbooks:**
Expand the existing Ransomware Playbook into tailored guides for high-risk sectors such as healthcare, education, and critical supply chains, providing actionable steps for prevention, detection, and recovery.

**National Simulation Exercises:**
Launch a Ransomware Exercise Program with AI-driven or scenario-based simulations to test incident response across SMEs, NFPs, and critical industries. This builds readiness, identifies gaps, and improves coordination between public and private sectors.

**Financial Incentives and Cyber Hygiene Vouchers:**
Introduce subsidies, grants, or tax credits for SMEs/NFPs implementing baseline protections, like Essential Eight controls, multi-factor authentication, and passwordless authentication. This lowers cost barriers and encourages widespread adoption.

**Centralised Ransomware Resource Portal:**
Develop a national portal providing access to decryption tools, reporting procedures, incident guidance, and case studies, similar to Singapore's ransomware initiatives. A single trusted source ensures timely, practical support for victims and responders.

**Mandatory Minimums in Supply Chains:**
Require vendors to government or critical infrastructure sectors to meet baseline cyber hygiene standards, creating a market-driven incentive for SMEs to adopt protective measures.

Ransomware attacks increasingly target small entities and critical sectors using sophisticated techniques, including AI-enabled phishing and automated exploitation. Sector-specific guidance ensures relevance, while simulation exercises build practical response skills. Financial incentives and vouchers address resource limitations, improving uptake of essential controls. Centralised portals and mandatory hygiene standards create trusted, consistent frameworks for prevention and rapid response, collectively enhancing national resilience against ransomware threats.

| | |
|---|---|
| **3.1.14** | 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? |

**Human Vulnerabilities:**
Certain communities, including seniors, Indigenous Australians, rural populations, and NFPs, are disproportionately affected due to limited cyber awareness, reliance on outdated devices, and minimal technical expertise. These factors increase susceptibility to phishing, AI-driven social engineering, and deepfake scams targeting trust and finances.

**Technical Vulnerabilities:**
Exposed services, unpatched remote access tools, and misconfigured cloud or IoT devices exacerbate risk. In NFPs, handling sensitive client or donor data without dedicated IT staff further heightens exposure to ransomware, fraud, and data breaches.

**Community Cyber Resilience Program (Recommended Interventions):**

**Co-Designed Vulnerability Assessments:** Use frameworks like NIST IR 8286 with community leaders to identify unique local threat patterns, such as elder scams or culturally sensitive data exploitation.

**Culturally Adapted Toolkits:** Simplify ASD Essential Eight controls into visual, audio, or local-language resources, extending Horizon 1's Cyber Wardens model for grassroots engagement.

**Rapid-Response Networks:** Partner with regional ISPs and banks to freeze suspicious transactions, leveraging infrastructure like the Small Business Cyber Resilience Service.

Disproportionate impacts arise where human and technical vulnerabilities intersect. Seniors, remote communities, and resource-constrained NFPs often lack proactive protections and accessible guidance. Co-designed assessments, culturally appropriate toolkits, and rapid-response mechanisms create targeted, practical defences, enabling communities to anticipate, detect, and respond to threats effectively. This approach ensures resilience is inclusive and addresses the specific risks faced by vulnerable cohorts.

| | |
|---|---|
| **3.1.15** | How can support services for victims of identity crime be designed to be more effective in the context of increasing demand? and |

To improve support services for victims of identity crime amidst rising demand, a three-tiered approach leveraging Horizon 1 infrastructure is recommended. First, an Automated Triage & Recovery Portal integrated into Cyber.gov.au would provide AI-driven credential freezing, step-by-step recovery plans, and secure verification using NIST SP 800-63 digital identity guidelines. Second, Community First Responders, such as trained Cyber Wardens, would offer in-person assistance to vulnerable populations like seniors or remote communities, extending Horizon 1's grassroots engagement model. Third, a Public-Private Threat Clearinghouse would enable real-time sharing of identity compromise patterns among banks, ASIC, and the ATO, improving detection and prevention while building on SOCI Act collaboration.

**Automated Recovery Portal:**
AI-powered tools streamline identity restoration, enabling instant credential freezing, secure verification, and guided recovery plans for individuals under attack.

**Community First Responders:**
Local volunteers provide hands-on support for vulnerable populations, bridging gaps in remote or underserved regions.

**Threat Clearinghouse:**
Real-time collaboration among banks, ASIC, and ATO enables early detection, shared intelligence, and coordinated responses to emerging identity crime patterns.

**NIST-Aligned Verification:**
Digital identity standards ensure secure authentication and interoperability, enhancing trust in automated support services.

**Scalable, Multi-Tiered Support:**
Combining technology, local engagement, and cross-sector intelligence addresses rising demand while maintaining timely, effective assistance for victims.

Identity crime is growing in scale and complexity, disproportionately affecting vulnerable populations such as seniors and regional communities. Existing services are fragmented, creating delays in detection, remediation, and cross-sector intelligence sharing. A three-tiered approach addresses these gaps: AI-powered portals automate immediate recovery, reducing reliance on human resources while maintaining secure verification via NIST SP 800-63 guidelines. Community First Responders extend support to underserved populations, ensuring equitable access and personalized guidance. A Public-Private Threat Clearinghouse promotes real-time intelligence sharing, allowing financial institutions and regulators to detect trends, prevent escalation, and coordinate responses. Together, these measures create a scalable, interoperable, and community-aware ecosystem, improving response times, increasing public trust, and reducing the operational and financial impact of identity crime for individuals and organisations alike.

## Consultation on developing Horizon 2

| 3.1.16 | Which regulations do you consider most important in reducing overall cyber risk in Australia? |
|---|---|

To holistically reduce cyber risk, Australia should prioritise regulations that address emerging threats, ensure compliance, and enhance cross-sector resilience. Key regulations include the Security of Critical Infrastructure (SOCI) Act 2018, which mandates risk management programs, supply chain security, and prompt incident reporting for critical sectors, with recent amendments extending obligations to cloud providers and MSPs. The Cyber Security Act 2024 establishes mandatory security standards for IoT devices, requires manufacturer compliance declarations, and enforces ransomware reporting. The Privacy Act 1988, including the Mandatory Data Breach Notification Scheme, strengthens protections for personal data, regulates cross-border flows, and aligns with GDPR-like standards. Additional enhancements include APRA CPS 234 expansions to cover fintech providers and mandatory AI governance for high-impact systems under NIST AI RMF guidance. Collectively, these regulations create a cohesive, interoperable, and forward-looking regulatory ecosystem that addresses technology, infrastructure, and data risks, while supporting national cyber resilience and international alignment.

**SOCI Act:**
Expands critical infrastructure obligations to cloud and MSPs, enforces risk management programs, incident reporting, and supply chain security, protecting vital national services.

**Cyber Security Act 2024:**
Establishes IoT security baselines, mandates manufacturer compliance, and enforces ransomware reporting, reducing vulnerabilities across connected devices.

**Privacy Act 1988:**
Implements strict personal data protections, mandatory breach notifications, and cross-border restrictions, enhancing trust and security in data handling.

**APRA CPS 234 & Fintech Updates:**
Strengthens financial sector resilience by mandating cloud security guidance and covering third-party fintech providers.

**AI Governance:**
Enforces mandatory risk assessments for high-impact AI systems, ensuring responsible deployment and mitigating emerging technology threats.

Australia faces a rapidly evolving cyber landscape, with emerging threats from cloud services, AI, IoT, and critical infrastructure supply chains. Strengthening regulations ensures consistent, enforceable cybersecurity practices across sectors and mitigates gaps exposed in Horizon 1. The SOCI Act provides a foundation for critical infrastructure protection, while Cyber Security Act 2024 addresses IoT vulnerabilities and ransomware. Privacy Act reforms enhance personal data protection, increasing organisational accountability and public trust. APRA CPS 234 expansions ensure financial sector resilience against third-party and cloud-related risks, while AI governance frameworks proactively address risks from generative and high-impact AI systems. Harmonising these regulations with international standards like NIST, ISO/IEC 62443, and GDPR ensures interoperability, reduces

## Consultation on developing Horizon 2

compliance complexity, and supports cross-border collaboration. Prioritising these measures creates a cohesive regulatory ecosystem, improving national cyber resilience and reducing systemic risk.

| | |
|---|---|
| **3.1.17** | Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues? |

Multiple, overlapping requirements, SOCI Act, APRA CPS 234, ISM, ASD Essential Eight, and Privacy Act obligations, can create complexity, confusion, and increased administrative overhead. Organisations often face duplicative reporting, inconsistent intervals, and fragmented guidance, which can slow operational improvements and divert resources from practical security activities.

**Management Strategies:**
Crosswalk Mapping: Develop a controls crosswalk to align regulatory requirements with operational security controls, showing where SOCI, CPS 234, ISM, and Essential Eight overlap.

**Operational Integration:**
Embed compliance activities into existing security maturity programs rather than treating them as separate audits, reducing duplication and ensuring actionable improvements.

**Risk-Based Prioritisation:**
Focus on high-impact controls and regulatory obligations to balance compliance with practical resilience, avoiding a checkbox mentality.

Monitoring and Reporting Automation: Implement tools to track control implementation and automate evidence collection to streamline reporting to multiple regulators.

Regulatory obligations, while critical for national cyber resilience, can inadvertently reduce organisational agility and security effectiveness when poorly harmonised. A crosswalk approach aligns multiple frameworks with operational controls, improving clarity, reducing redundancy, and ensuring that compliance activities directly contribute to improved cyber maturity. Embedding compliance within day-to-day operations ensures resources strengthen real security outcomes rather than solely fulfilling reporting requirements.

| | |
|---|---|
| **3.2.18** | 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? |

To strengthen secure technology standards, Australia can adopt internationally recognised frameworks tailored to IoT, CER, and OT environments. For IoT and CER, the ETSI EN 303 645 standard provides baseline security requirements, ensuring devices are resilient against common threats. Complementary guidance from CIS Controls for IoT offers actionable controls for consumer, enterprise, and industrial deployments. Countries like Singapore, Finland, and Germany have implemented IoT labelling schemes, classifying products from self-declaration to independent penetration testing, helping consumers and organisations make informed security choices. The forthcoming ISO/IEC 27404 standard will further harmonise labelling globally. For operational technology, ISO/IEC 62443 remains the benchmark for industrial automation and control systems, offering lifecycle-based security guidance and aligning with frameworks such as NIST CSF. Combining internationally recognised standards, labelling, and certification ensures a robust, interoperable, and consistent security posture for edge devices, CER, and OT in Australia.

**ETSI EN 303 645:**
Provides baseline security requirements for consumer IoT devices, covering areas like data protection, secure updates, and vulnerability disclosure. Adoption ensures minimum security standards are met across connected devices.

**CIS IoT Controls & Companion Guide:**
Offers practical, actionable controls for organisational, home, and industrial IoT environments, bridging the gap between policy and operational security.

**IoT Labelling Programs:**
Countries like Singapore, Finland, and Germany classify devices based on conformance, enhancing consumer awareness, market consistency, and adoption of secure practices.

**ISO/IEC 62443:**
Establishes cybersecurity standards for operational technology and industrial automation, addressing technical, procedural, and lifecycle aspects, closely aligned with NIST CSF.

**ISO/IEC 27404, Cybersecurity  IoT security and privacy (in final draft):**
Provides a harmonised international framework for IoT cybersecurity labelling, improving global interoperability, consumer understanding, and market trust.

Global best practices demonstrate that standards alone are insufficient without mechanisms for certification, labelling, and lifecycle management. ETSI EN 303 645 provides clear baseline requirements for IoT and CER devices, while CIS IoT Controls translate these into operational practices. Labelling programs in Singapore, Germany, and Finland help consumers and organisations quickly identify secure devices, encouraging market adoption and compliance. For operational technology, ISO/IEC 62443 delivers comprehensive guidance covering technical controls, policies, and procedures, ensuring security across industrial systems. The combination of international

standards, practical guidance, and certification frameworks enables Australia to mitigate systemic risks, enhance consumer confidence, and maintain alignment with global cybersecurity practices. Applying these standards across edge devices, CER, and OT will strengthen national resilience, reduce vulnerabilities in critical sectors, and support consistent, measurable security outcomes. We acknowledge the effort of the Australian Government in adopting ISO/IEC 62443 as its national framework for securing operational technology (OT) in critical infrastructure in July 2025. This has set out clear regulatory expectations for OT cybersecurity across essential sectors.

| | |
|---|---|
| **3.2.19** | 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? |

To better inform consumers and end-users about cybersecurity, the government should leverage Horizon 1 foundations such as Cyber.gov.au and the Cyber Wardens Program. A coordinated approach would include expanding unified awareness campaigns that provide standardized, globally-aligned (NIST/ISO) cyber hygiene guidance, translated into accessible formats for diverse audiences. Consumer-facing initiatives can be strengthened by integrating cybersecurity advice into product labelling and retail touchpoints, ensuring users see actionable guidance at the point-of-sale. The Small Business Cyber Resilience Service can be scaled to include modules for individuals and households, such as "Cyber Check" self-assessments that highlight practical steps to mitigate risk. Finally, threat intelligence sharing should be tailored to non-technical users through plain-language bulletins and SMS/email alerts, providing timely, relevant information about emerging threats like ransomware or phishing campaigns. These combined measures enhance awareness, trust, and protective behaviour across the community.

**Unified Awareness Campaigns:**
Centralised, standardized guidance aligned with global standards, translated for diverse audiences, increases accessibility and reduces confusion about cyber hygiene practices.

**Product Labelling & Retail Integration:**
Embedding security tips into IoT labelling and point-of-sale interactions helps consumers make informed choices about secure devices.

**Scaled Cyber Resilience Service:**
Expanding self-assessment modules for consumers and SMEs empowers individuals and businesses to identify risks and take practical protective measures.

**Plain-language Threat Bulletins:**
Timely SMS/email alerts about emerging threats, simplified for non-technical users, enable rapid understanding and response to cyber incidents.

Consumers and end-users often face complex cybersecurity challenges but lack accessible guidance. Horizon 1 initiatives demonstrated the value of centralised resources, but fragmented messaging can reduce uptake. Standardising advice across Cyber.gov.au, translated into plain language, ensures clarity and wider accessibility. Integrating guidance into product labels and retail points creates direct touchpoints for actionable information. Scaling the Small Business Cyber Resilience Service to include consumer modules allows individuals to self-assess and improve security in a structured, measurable way. Tailored threat bulletins delivered via SMS/email provide real-time updates, reinforcing awareness and promoting proactive behaviour. Together, these interventions create a cohesive, practical framework for consumers to understand and mitigate risks, improve adoption of secure practices, and foster a more cyber-resilient population.

| | |
|---|---|
| **3.3.20** | What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors? |

To better manage Foreign Ownership, Control, or Influence (FOCI) risks among technology vendors, the government should build on Horizon 1's initiatives such as Cyber.gov.au and the Cyber Wardens Program. Establishing a standardized FOCI Risk Assessment Framework aligned with global benchmarks (e.g., NIST SP 800-171/172, ISO 27036-3) provides clarity and consistency, with sector-specific guidance for critical infrastructure, SMEs, and NFPs. A centralized Technology Vendor Review Portal would enable real-time threat intelligence, track high-risk vendors and leverage coordinated national oversight. For SMEs and NFPs, practical toolkits, including simplified checklists, contract templates, and Essential Eight-aligned guidance, would replicate the accessible, grassroots approach of Cyber Wardens, helping smaller organisations address vendor-related risks effectively. This approach ensures all entities can consistently identify, assess, and respond to FOCI-related threats, improving national cyber resilience while supporting practical compliance measures.

**FOCI Risk Assessment Framework:**
Standardized, globally-aligned framework reduces inconsistencies, providing actionable guidance for evaluating foreign influence across critical infrastructure, SMEs, and NFPs.

**Technology Vendor Review Portal:**
Centralized platform offering real-time intelligence on high-risk vendors enhances transparency, coordination, and proactive mitigation of supply chain threats.

**SME/NFP Toolkits:**
Accessible checklists and templates based on Essential Eight replicate Cyber Wardens' grassroots approach, enabling smaller entities to manage vendor risks efficiently.

Managing FOCI risks is complex, particularly for SMEs and NFPs lacking internal security expertise. Horizon 1 revealed inconsistencies in terminology and fragmented guidance, reducing confidence in risk assessments. A globally-aligned framework ensures consistent evaluation standards and supports interoperability with international best practices. Centralized threat intelligence provides timely alerts on vendor risks, allowing organisations to act before supply chain issues escalate. Toolkits for SMEs and NFPs bridge capability gaps by offering practical, digestible resources that do not require specialist knowledge. By combining standardization, real-time intelligence, and accessible tools, the government can support a tiered, scalable approach to managing FOCI risks, reducing the likelihood of supply chain compromises and reinforcing national cyber security across diverse organisational contexts.

| | |
|---|---|
| **3.2.23** | What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies? |

To ensure safe and responsible uptake of critical and emerging technologies, the government should implement a Critical Technologies Assurance Framework. This framework would provide risk-based, sector-specific guidance, using internationally recognised standards such as NIST AI RMF and ISO/IEC 23053, tailored for SMEs with practical checklists available via Cyber.gov.au. Sandbox environments monitored by ASD could allow innovators to test technologies such as quantum computing and blockchain under controlled conditions, offering limited regulatory waivers for compliant participants, building on Horizon 1 Cyber Security Act 2024 pilot provisions. Additionally, ethical procurement standards for government vendors should require adherence to the Essential Eight and OECD AI Principles, leveraging the Horizon 1 Technology Vendor Review Framework. This approach balances innovation with safety, ensuring emerging technologies are implemented securely, responsibly, and consistently across sectors, while also supporting SMEs and start-ups in aligning with best practices from the outset.

**Risk-Based Guidelines:**
Sector-specific guidance for critical technologies, providing SMEs and larger organisations with actionable standards and compliance checklists based on NIST AI RMF and ISO/IEC 23053, enhancing secure adoption.

**Sandbox Environments:**
Controlled testbeds monitored by ASD, allowing safe experimentation with emerging technologies such as quantum computing and blockchain while providing limited regulatory flexibility for compliant innovators.

**Ethical Procurement Standards:**
Mandates government vendors adhere to Essential Eight controls and OECD AI Principles, embedding ethical and secure practices in technology adoption and reinforcing national cybersecurity norms.

Emerging technologies introduce significant opportunities but also create novel cybersecurity, privacy, and ethical risks, especially for SMEs and public sector adoption. Risk-based guidance ensures sector-specific adoption strategies are practical and aligned with international best practices, reducing inconsistencies and improving security maturity. Sandbox environments provide a low-risk space for experimentation, allowing innovation while mitigating systemic threats. Ethical procurement standards embed security and responsible design at the point of purchase, ensuring that critical government and industry technologies meet national cyber and ethical benchmarks. Together, these measures encourage innovation without compromising safety, support SMEs in compliance, and create consistent adoption pathways across sectors. By combining technical guidance, practical testing, and procurement incentives, the government can cultivate a trusted ecosystem for critical technologies that balances progress, safety, and ethical responsibility, directly addressing gaps identified in Horizon 1.

| | |
|---|---|
| **3.3.24** | 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? |

To support and empower industry to take a proactive cyber security posture, the government should establish a Proactive Cyber Partnership Program. This program would enable real-time threat intelligence sharing through upgraded Cyber.gov.au feeds, aligned with STIX/TAXII standards, and incentivise SME participation via tax rebates for joining ISACs or adopting ASD threat-sharing protocols. Skills mobilisation should be enhanced by deploying Cyber Reserve Teams, trained professionals standing by to assist during sector-wide incidents, leveraging the ASD Cyber Skills Framework and mirroring Horizon 1's RAPID model. Australia's ideal proactive posture for industry should balance autonomy with oversight, allowing businesses to lead threat disruption while ASD provides legal and technical guidance. Resources should prioritise pre-breach mitigation (targeting 80% of effort), and actions should be sector-tailored, with energy focusing on operational technology resilience and finance emphasising fraud prevention. This approach strengthens national cyber resilience by combining industry expertise, government coordination, and incentivised participation. Threat Intelligence Sharing 2.0 – Real-time, automated, machine-readable threat feeds accessible via Cyber.gov.au, enabling industry to block threats proactively, while SMEs receive tax incentives for ISAC participation and adopting standardized threat-sharing protocols.

**Skills Mobilisation:**
Cyber Reserve Teams of vetted professionals on standby, ready to assist during sector-wide cyber incidents, ensuring rapid response and knowledge transfer across industries, using ASD's Cyber Skills Framework as a competency standard.

**Proactive Posture for Industry:**
Prioritises prevention over reaction (80% pre-breach focus), balances autonomy with government oversight, and tailors strategies to sector-specific risks, reinforcing resilience across energy, finance, and other critical sectors.

Industry plays a pivotal role in national cyber resilience but often lacks resources, standardised intelligence, and access to skilled responders. By upgrading threat intelligence sharing, the government can empower businesses to act in real time, reducing breach impacts and improving situational awareness. Skills mobilisation via Cyber Reserve Teams addresses workforce shortages and provides rapid, industry-aligned support during incidents. A proactive posture focusing on prevention ensures resources target vulnerabilities before exploitation, rather than predominantly reacting post-breach. Sector-specific approaches allow tailored interventions, optimising resilience in critical areas like operational technology, fraud detection, and supply chain security. Incentivising participation through tax rebates and collaborative ISAC engagement encourages industry ownership of cyber security, while ASD oversight ensures legal compliance and technical alignment. Together, these measures create a cohesive, forward-looking ecosystem that strengthens Australia's national cyber posture and reduces systemic risk.

| 3.3.26 | How could government further support industry to block threats at scale? |
|---|---|

To support industry in blocking cyber threats at scale, the government should establish a National Threat Blocking Framework leveraging ACSC as the coordinating authority. Key actions include collaborating with ISPs to implement DNS-based blocking of known malicious domains for government agencies, critical infrastructure, and subscribing businesses, enabling consistent, large-scale protection. ACSC should also engage the global security community to identify malicious network blocks in the APAC region, working with APNIC to regulate or neutralise these blocks. Public URL and IP blocklists could be maintained and made available via subscription, allowing modern home routers, enterprise firewalls, and cloud security platforms to dynamically enforce blocking rules. This approach extends Horizon 1's threat intelligence initiatives into operational, real-time mitigation, ensuring smaller businesses and distributed networks benefit from collective protection and reducing the likelihood of lateral spread from high-risk traffic.

The Government, via ACSC, should partner with ISPs to implement DNS blocking of known malicious domains for government agencies, critical infrastructure, and subscribing businesses. This ensures consistent, large-scale threat mitigation across multiple sectors.

ACSC can engage with the global security community to detect network blocks in the APAC region used by cybercriminals. Collaborating with APNIC to regulate or mitigate these blocks strengthens regional cybersecurity posture.

ACSC can offer publicly accessible URL blocklists that modern home routers and enterprise firewalls can subscribe to. Automatic updates allow dynamic blocking of malicious hyperlinks, protecting both consumers and organisations in real time.

A centralised, government-coordinated approach to threat blocking ensures uniform protection across sectors, leveraging national-scale visibility that individual organisations cannot achieve. DNS and URL-based blocking are proven, low-cost methods to reduce exposure to phishing, malware, and command-and-control infrastructure. Collaboration with APNIC and global security communities ensures rapid identification of emerging threats, while subscription-based blocklists allow automated enforcement without requiring specialised in-house teams. By extending threat intelligence into actionable, real-time controls, the framework protects smaller and resource-constrained organisations, aligns with international best practices, and builds a more resilient national cyber ecosystem capable of pre-empting attacks before they propagate.

| | |
|---|---|
| **3.3.27** | How could the use of safe browsing and deceptive warning pages be amplified? |

ACSC should collaborate with major browser vendors to amplify the safe browsing initiative. Integrating threat intelligence directly into browsers ensures users receive real-time warnings and information when attempting to access malicious websites.

Beyond simply blocking access, warning pages should provide clear, concise details about the threat type, potential impact, and recommended user actions. This educates users while preventing unsafe interactions with harmful sites.

Amplifying safe browsing and deceptive warning pages strengthens the proactive defence posture for both individuals and organisations. Browser integration allows warnings to reach users at the point of exposure, reducing the likelihood of successful attacks. By providing actionable information on deceptive warning pages, users gain awareness of specific risks, enabling safer online behaviour and reducing reliance solely on automated controls. Collaboration with security platforms ensures that threat intelligence is current, relevant, and contextualised for diverse threat types. This approach also supports industry-wide standards for user protection, creating consistency across platforms and enhancing trust in online environments. Ultimately, combining technical blocking with informative guidance fosters a more cyber-aware population and reduces the impact of social engineering and malware campaigns at scale.

| | |
|---|---|
| **3.3.28** | 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? |

The Australian Government should support the creation of Information Sharing and Analysis Centres (ISACs) tailored to low-maturity sectors, such as healthcare and agriculture. These ISACs would provide a central hub for threat intelligence sharing and guidance.

Offer user-friendly threat intelligence platforms and resources that cater to the needs of low-maturity sectors. This includes simplified dashboards, automated threat feeds, and educational materials to enhance cybersecurity awareness and capabilities.

Encourage collaborations between government agencies, industry associations, and private sector entities to provide cybersecurity support and resources to low-maturity sectors. These partnerships can facilitate knowledge sharing and capacity building.

Low-maturity sectors often lack the internal resources and expertise to effectively participate in traditional ISACs. By establishing sector-specific ISACs, these industries can receive tailored support and guidance, enabling them to improve their cybersecurity posture. Providing accessible threat intelligence tools ensures that organizations can understand and act upon relevant threats without requiring advanced technical skills. Public-private partnerships can bridge the resource gap, offering mentorship, training, and shared resources to bolster cybersecurity efforts in these sectors. These initiatives align with the Australian Government's commitment to enhancing cybersecurity resilience across all sectors, as outlined in the 2023–2030 Australian Cyber Security Strategy.

| | |
|---|---|
| **3.3.30** | 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? |

The Government should take primary responsibility for managing major cyber security incidents, coordinating resources, and liaising with all relevant stakeholders to mitigate potential impacts. Clear leadership ensures rapid, centralised decision-making during crises.

ACSC should coordinate sector-specific cyber drills for critical infrastructure. These exercises simulate realistic cyber conflict or crisis scenarios, enabling organisations to practice response procedures, communication protocols, and collaboration with government agencies.

Exercises should include the latest threat intelligence and crisis developments to reflect the current cyber landscape. This ensures participants gain practical experience in dealing with modern attack vectors and evolving tactics.

Clear delineation of roles between government and industry is crucial during cyber conflicts or crises to prevent confusion, duplication, or delays in response. Government leadership provides central oversight and ensures coordination of resources, while industry participation ensures operational continuity. Cyber exercises allow organisations to test and refine their incident response plans, improve coordination with government entities, and familiarise staff with procedures in high-pressure scenarios. Incorporating emerging threat scenarios ensures that exercises remain relevant, preparing participants for contemporary attack methods and tactics used by adversaries. Collectively, these measures enhance resilience, build trust between public and private sectors, and ensure a more agile and coordinated response to cyber crises, reducing potential damage and improving recovery outcomes across critical infrastructure and essential services.

| | |
|---|---|
| **3.3.31** | How could government better incentivise businesses to adopt vulnerability disclosure policies? |

Governments could provide matching funds or tax incentives to organisations that run private or public bug bounty programs. This reduces the financial burden of proactive security research and encourages businesses to invest in identifying and resolving vulnerabilities.

By collaborating with cybersecurity vendors and industry groups, the government can sponsor bug bounty competitions. Offering tangible rewards through these programs motivates ethical hackers to report vulnerabilities via responsible disclosure channels.

Public recognition, awards, or cyber security excellence accolades for organisations and researchers can highlight best practices. Celebrating achievements fosters a culture of responsible reporting and incentivises businesses to adopt robust vulnerability disclosure policies.

Incentivising businesses to implement vulnerability disclosure policies encourages a proactive approach to cybersecurity, reducing the risk of exploitation. Financial support and tax benefits lower the cost barrier for running bug bounty programs, making security research economically viable. Sponsoring competitions engages ethical hackers, ensuring vulnerabilities are identified and reported responsibly rather than exploited maliciously. Recognition through awards or public acknowledgement not only motivates organisations and researchers but also raises awareness of cybersecurity best practices across industries. Together, these measures create a culture that values proactive vulnerability management, strengthens collaboration between industry and government, and increases overall cyber resilience. By combining monetary, reputational, and collaborative incentives, the government can accelerate the adoption of responsible disclosure frameworks, improving detection and mitigation of threats before they impact businesses and the broader community.

| | |
|---|---|
| **3.3.32** | Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities? |

Australia should explore creating a coordinated vulnerability disclosure program. This would provide security researchers with a clear, safe mechanism for reporting vulnerabilities directly to a central authority, such as ASD, for validation and follow-up.

Coordinated disclosure practices would bring Australia in line with global standards, enhancing trust between researchers, organisations, and government. It supports a resilient cybersecurity ecosystem by ensuring vulnerabilities are addressed before exploitation.

By proactively managing reports, acknowledging submissions, and coordinating remediation with affected organisations, ASD can incentivise researchers to continue contributing their time and expertise, including in smaller organisations that may otherwise ignore reports.

Australia has a strong community of ethical hackers and threat hunters, yet many are discouraged from reporting vulnerabilities due to a lack of acknowledgement or effective follow-up. Current channels, such as the ASD Cyber Security Reporting portal, mainly redirect to OAIC for data breaches, leaving a gap for reporting technical vulnerabilities. A national program would centralise intake, validate reports, and coordinate remediation with organisations, improving both responsiveness and accountability. Aligning with international best practices ensures Australia benefits from established frameworks while building trust with researchers. Proactive engagement encourages continued volunteer contributions, particularly for smaller entities that lack mature security processes. Overall, a coordinated vulnerability disclosure program strengthens national cyber resilience, incentivises responsible reporting, and ensures that critical vulnerabilities are addressed efficiently, reducing potential exploitation and enhancing the security posture of both public and private sectors.

| | |
|---|---|
| **3.4.34** | Are there significant cyber security risks that are not adequately addressed under the current framework? |

Current frameworks insufficiently cover risks from foreign adversaries, third-party suppliers, and upstream vendors. Organisations need enhanced integration with international supply chain security standards and participation in global information-sharing bodies to collaboratively mitigate geopolitical and supply chain threats.

While incident reporting exists, the timely sharing of actionable threat intelligence for proactive defence is limited. Legal protections and incentives are needed to encourage organisations to share threat data and indicators in real time.

Industry-focused Information Sharing and Analysis Centres (ISACs) can facilitate real-time intelligence exchange and collaborative response among critical infrastructure sectors. These bodies should be supported with appropriate legal frameworks, governance, and incentives to ensure organisations actively participate.

Significant cyber risks remain inadequately addressed under the current framework, particularly those arising from complex supply chains and international geopolitical pressures. Traditional third-party vendor management only partially mitigates upstream risks, leaving organisations exposed to indirect vulnerabilities. Aligning with international standards and collaborative information-sharing frameworks allows for more comprehensive, proactive risk management. Similarly, reactive incident reporting does not provide sufficient time for preventive action. Establishing ISACs for critical infrastructure, combined with legal protections and incentive mechanisms, encourages organisations to share timely, actionable intelligence that can prevent attacks or reduce impact. Together, these measures strengthen national resilience, support collaborative defence, and ensure that both government and industry can respond effectively to emerging cyber threats in a rapidly evolving geopolitical and technological landscape.

| | |
|---|---|
| **3.4.35** | Is the regulatory burden on industry proportionate to the risk and outcomes being sought? |

The SOCI framework's complexity can disproportionately burden smaller critical asset owners. A tiered approach, where compliance requirements are scaled based on asset criticality and organisational capacity, would reduce unnecessary complexity while maintaining robust security standards.

Smaller organisations often struggle to interpret and implement regulatory requirements. Government-led outreach programs and technical guidance can support risk assessment, remediation planning, and practical implementation of controls.

Funding advisory programs helps smaller critical asset owners access expert advice without incurring prohibitive costs. This ensures they can achieve compliance effectively while mitigating cyber risks in line with national objectives.

While the SOCI framework aims to secure critical assets, its complexity can create an uneven regulatory burden, particularly for smaller organisations with limited resources. A tiered, scalable approach ensures that compliance expectations are proportional to risk, enabling organisations to focus on the most critical controls. Targeted outreach and technical guidance help bridge knowledge gaps, providing practical assistance in risk assessment and remediation. Government-funded advisory programs further support smaller entities by offering access to expertise that may otherwise be unaffordable, reducing compliance friction and promoting consistent security outcomes. By balancing regulatory rigour with proportional support, the government can achieve its cybersecurity objectives while minimising unnecessary burden, ensuring that all critical asset owners, regardless of size, can effectively protect their systems and contribute to national cyber resilience.

| | |
|---|---|
| **3.4.37** | How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls? |

The Government should fund TAFE courses, online training modules, and professional certifications tailored to different sectors and organisational sizes. These programs should cover both international and Australian security certifications, regulatory requirements, and relevant technical controls to build sector-specific capability.

Government can lead by example, incorporating required security certifications and adherence to technical controls into procurement tenders, contracts, and job recruitment criteria. This sets clear expectations for private sector partners and incentivises compliance with national security standards.

Supporting private sector engagement requires both capability building and clear expectations. By investing in workforce development, the government equips organisations with the knowledge and skills necessary to implement security controls and meet regulatory requirements. Tailored training ensures relevance for organisations of varying sizes and sectors, improving overall cybersecurity maturity. Simultaneously, embedding security certification and technical control requirements into tenders and recruitment signals the importance of compliance and creates a tangible incentive for private sector partners to adopt best practices. Together, these measures strengthen collaboration between government and industry, enhance national cyber resilience, and encourage a culture of compliance. They ensure that organisations are both capable and motivated to meet government security requirements, reducing risk across critical infrastructure and sensitive sectors while aligning with international and domestic security standards.

| | |
|---|---|
| **3.4.38** | How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure? |

Adoption of Australian Government security frameworks among private sector partners, particularly SMBs, remains inconsistent. Smaller organisations often lack the resources and skilled personnel to implement required security controls effectively, leaving gaps in compliance and resilience.

Government could collaborate with selected MSSPs to deliver affordable, simplified security solutions tailored for SMBs. This approach enables smaller organisations to uplift their security maturity and better align with national frameworks without bearing the full operational burden.

While large organisations and critical infrastructure operators may have the capacity to implement government security requirements, SMBs frequently face resource and skill constraints. This results in uneven adoption and potential vulnerabilities within critical sectors. Engaging MSSPs provides a practical solution, offering SMBs access to expert-managed security services that implement controls consistent with Australian Government standards. Such partnerships reduce the operational and financial barriers for smaller organisations while ensuring compliance and improving national cyber resilience. By simplifying adoption through managed services, the government can extend the reach of its security frameworks, standardise practices across sectors, and ensure that even resource-limited businesses contribute effectively to the protection of critical infrastructure and national cybersecurity objectives.

| | |
|---|---|
| **3.5.39** | 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? |

The Government should establish a coordinated program combining vocational training, university partnerships, and industry placements to rapidly scale Australia's cyber workforce. This program would provide structured pathways for learners at all levels, from beginners to expert practitioners.

Subsidised apprenticeships should support mid-career transitions and job seekers, helping them gain globally recognised certifications such as CISSP, CISM, or CREST. Diversity scholarships should target women, First Nations students, regional Australians, and underrepresented groups, building an inclusive and skilled cyber workforce.

A Cyber Skills Passport recognising micro-credentials aligned with the ASD Cyber Skills Framework and international standards would formalise workforce competencies. Professional certifications compliant with ISO/IEC 17024 can further professionalise the sector and ensure global alignment.

Australia faces a significant shortage of skilled cybersecurity professionals, which threatens national resilience and the ability to meet emerging threats. The ASD Cyber Skills Framework provides a foundation, but scaling capability requires structured programs that integrate training, practical experience, and professional recognition. Subsidised apprenticeships and scholarships make pathways accessible to diverse populations, addressing workforce gaps and promoting inclusion. The Cyber Skills Passport and professionalisation scheme formalise skills recognition, aligning with international standards and promoting career progression. Globally recognised certifications ensure Australian professionals can compete internationally and adapt to rapidly evolving threats. Collectively, these initiatives foster a sustainable, high-quality cybersecurity workforce, enabling both government and industry to strengthen national cyber resilience while ensuring Australia remains competitive in the global cybersecurity market.

| | |
|---|---|
| **3.5.40** | 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? |

Programs like Ready Cyber, co-designed by ASD and industry, provide intensive bootcamps that help mid-career professionals transition into cybersecurity roles. Using the ASD Cyber Skills Framework ensures training aligns with high-priority roles such as incident responders, improving workforce readiness.

Initiatives such as Tech Ready Women and Indigenous Cyber Careers offer paid internships and community partnerships to place women and First Nations participants into cyber roles. These programs build inclusive pipelines and address systemic barriers to STEM and cybersecurity careers.

Proven initiatives for mid-career transitions and diversity combine targeted skills mapping, structured training, and mentorship to address gaps in Australia's cybersecurity workforce. Programs like Ready Cyber provide a fast-track into critical roles, enabling experienced professionals to pivot effectively and meet industry demand. Diversity-focused accelerators ensure underrepresented groups have access to pathways, mentorship, and practical experience, addressing inequities while expanding the talent pool. Aligning all programs with the ASD Cyber Skills Framework guarantees that the skills acquired are relevant and recognised across industry and government. Scaling these initiatives increases workforce capacity, strengthens inclusion, and supports national cyber resilience by ensuring a broader and more diverse talent pool equipped to respond to evolving threats. These approaches provide practical, scalable models for integrating both mid-career professionals and underrepresented populations into cybersecurity and STEM fields.

| | |
|---|---|
| **3.5.41** | 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? |

Certain industries provide a strong foundation for rapid integration into the cybersecurity workforce. Local cyber NFP communities excel in security awareness training and communication, filling gaps in education and "translator" roles between technical and non-technical teams. Network engineers and system administrators possess infrastructure security knowledge, enabling them to pivot into penetration testing, cloud security, or IT security operations. Auditors and fraud investigators bring expertise in risk governance and compliance, well-suited for GRC or fraud detection roles. Reports from Tech Council Australia (2024) and ACS Australia (2023) highlight the high demand for these capabilities and indicate that 68% of cyber hires originate from adjacent IT roles.

Government and industry should support training programs that integrate OT cybersecurity, IT security, and AI competencies, alongside cross-sector research grants and innovation challenges. This approach fosters skill transfer, collaboration, and the creation of tools and frameworks for securing critical infrastructure.

Rapidly expanding the cyber workforce requires tapping into existing pools of skilled professionals. Adjacent sectors such as IT, auditing, fraud investigation, and NFP cybersecurity education provide relevant experience that can be applied to critical cyber roles, reducing training time and accelerating readiness. Interdisciplinary programs combining OT, IT, and AI further expand capabilities, enabling professionals to address complex, interconnected threats in critical infrastructure and emerging technology environments. Research from ACS and Tech Council Australia supports this approach, demonstrating both the demand for transferrable skills and the success of leveraging adjacent industry expertise. By combining targeted reskilling, interdisciplinary pathways, and collaborative innovation, the government can effectively scale the cyber workforce, promote knowledge transfer, and strengthen national cyber resilience while ensuring that professionals can adapt to rapidly evolving threats and technological developments.

| | |
|---|---|
| **3.5.42** | 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? |

Australia should create a consortium involving government, academia, industry, and think tanks to coordinate cybersecurity research and innovation. This platform would provide a formal structure for collaboration and ensure alignment with national strategic, economic, and community interests.

Annual workshops led by ASD, CSIRO, and industry bodies such as AISA, ISC2, and ISACA can identify emerging strategic priorities like post-quantum cryptography and AI security. Using frameworks like NIST Cybersecurity Framework ensures consistent benchmarking and alignment across sectors.

Secondments between academia, industry, and government, alongside support for NFP cyber awareness missions, accelerate knowledge sharing and strengthen workforce capability. This builds on Horizon 1's Executive Cyber Council partnerships.

Sharing threat intelligence, tools, and research outputs via Cyber.gov.au encourages transparency, accelerates innovation, and integrates academic collaboration features into the national cybersecurity ecosystem.

Collaboration across government, industry, academia, and think tanks maximises Australia's cybersecurity innovation potential. A structured consortium enables joint priority setting, ensuring research efforts are strategically aligned with national interests. Horizon-scanning workshops provide a forward-looking approach, identifying critical emerging areas and reducing duplication of effort. Talent mobility programs foster cross-sector learning, accelerating skill development and the transfer of practical knowledge, while supporting NFP initiatives enhances community awareness and engagement. Open research repositories encourage transparency and collaboration, allowing tools, data, and intelligence to be shared efficiently, accelerating innovation and the adoption of best practices. Together, these actions create a coordinated ecosystem where strategic research, workforce development, and operational capability reinforce each other. This approach ensures Australia can respond to evolving cyber threats, foster innovation, and strengthen economic and community outcomes while maintaining international competitiveness and resilience.

| | |
|---|---|
| **3.5.43** | How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities? |

Australia should establish a structured program to strengthen links between government and academia, enabling direct collaboration on research and policy development in cybersecurity and emerging technologies.

Fund 12-month placements for academics within government policy teams (e.g., ASD, Home Affairs) and vice versa. These fellowships would focus on strategic areas such as AI governance or critical infrastructure security and use the ASD Cyber Skills Framework to align competencies, fostering practical understanding and skill transfer.

Expand Cyber.gov.au to include a portal offering standardized datasets (e.g., anonymized SOCI Act incident reports), policy brief templates aligned with NIST Special Publications, and a matchmaking tool to facilitate cross-sector collaborative projects.

Enhancing government-academia partnerships requires structured opportunities for people-to-people engagement and knowledge exchange. Embedded fellowships allow researchers and policymakers to gain firsthand experience, align academic insights with practical policy needs, and accelerate the translation of research into actionable strategies. A unified knowledge hub consolidates resources, provides accessible datasets, and standardizes reporting tools, enabling academics to contribute evidence-based insights while ensuring outputs meet government policy standards. The matchmaking functionality promotes interdisciplinary, cross-sector collaboration, fostering innovation and strengthening networks. Together, these initiatives increase research impact, cultivate a workforce skilled in both policy and technical domains, and improve national cybersecurity resilience. By formalizing these collaborative mechanisms, Australia can build stronger relationships between academia and government, support informed policy-making, and accelerate research translation to address emerging cyber challenges effectively.

| | |
|---|---|
| **3.5.45** | What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore? |

Telecommunications providers, in partnership with government, should establish clean pipe services that block malicious IP segments and filter high-volume attacks like DDoS before they reach end users. This reduces the operational burden on smaller organisations and critical service operators while improving national cyber resilience.

Government and providers should continuously monitor Border Gateway Protocol (BGP) routes to detect and mitigate hijacking attempts, which can redirect or intercept traffic at scale. Early detection safeguards communications and prevents widespread disruption.

Encourage multiple providers, diverse routing paths, and robust interconnections to reduce dependency on single providers. Mandating minimum network security standards across providers ensures baseline protections against cyber and operational risks.

High ICT concentration creates systemic vulnerabilities, where attacks or failures affecting a single provider can cascade across multiple organisations and sectors. Clean pipe services proactively block malicious traffic, alleviating the burden on smaller entities that lack advanced network defenses. Monitoring BGP routes mitigates emerging threats from traffic hijacking, a significant risk for national infrastructure. Strengthening redundancy and diversifying network paths reduces single points of failure, ensuring continuity of critical services even if one provider is compromised. Mandating baseline security standards ensures all providers maintain minimum protections, raising the overall resilience of national ICT infrastructure. Together, these mitigation strategies address both technical and operational concentration risks, distributing risk across multiple providers, reducing exposure to large-scale cyber attacks, and safeguarding the continuity and integrity of essential communications and services.

| | |
|---|---|
| **3.6.46** | 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? |

Public attribution of malicious activity, timely advisories, and targeted sanctions remain essential tools for deterring cyber threats. They hold malicious actors accountable, reinforce international norms, and signal consequences for attacks against Australia's national interests.

Australia should develop partnerships with ISPs, cloud providers, and other critical service operators to automatically disrupt known malicious infrastructure, including botnets and phishing domains. This approach leverages ASD threat intelligence and mirrors successful elements of the UK's Active Cyber Defence program, enabling faster, large-scale mitigation of cyber threats.

Combining technical disruption with diplomatic engagement, such as confidence-building measures, information-sharing agreements, and coordinated international responses, strengthens deterrence and encourages collective resilience against transnational cyber threats.

While attributions, advisories, and sanctions effectively influence state and non-state actors by establishing accountability, they are reactive measures and may not prevent immediate harm. Expanding the cyber deterrence toolkit with active defence partnerships allows Australia to disrupt malicious infrastructure before it impacts critical services or private organisations, providing proactive protection at scale. Collaborating with ISPs and cloud providers ensures that mitigation actions are timely and effective, while integration with ASD threat intelligence guarantees decisions are informed by credible data. Coupling these technical measures with diplomatic engagement reinforces international norms and promotes collective responsibility, creating both preventive and responsive deterrence. Collectively, this approach balances enforcement, proactive defense, and diplomacy, enhancing Australia's ability to counter evolving cyber threats in Horizon 2, safeguard national interests, and support resilience across critical infrastructure and the broader digital ecosystem.

| | |
|---|---|
| **3.6.47** | Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security? |

Australia should establish a regional partnership to strengthen cyber resilience across Southeast Asia and the Pacific. This program would coordinate activities, share intelligence, and align strategies to address cross-border cyber threats.

Biannual cross-border simulations with ASEAN and Pacific partners should focus on critical sectors such as ports and energy. Using ASD threat intelligence and Horizon 1's National Cyber Exercise Program as a model, exercises would include joint after-action reviews published on Cyber.gov.au, enabling learning and capability building.

Fund 12-month placements for Australian cyber specialists in partner nation CERTs, with reciprocal inbound placements to ASD. Establish regular forums or working groups for national CERTs to share best practices, coordinate incident response, and enhance regional collaboration.

Invest in programs like SEA-PAC Cyber, promote workforce development, real-time threat sharing, and initiatives such as IoT labelling programs in collaboration with Singapore, New Zealand, and Pacific Island countries.

Cyber threats are transnational, making regional collaboration essential. Shared exercises and real-time intelligence sharing enhance preparedness, harmonise response protocols, and build trust between partner nations. The Regional Cyber Fellows Program strengthens people-to-people links, promotes knowledge transfer, and cultivates skilled professionals capable of supporting regional resilience. CERT forums facilitate ongoing collaboration, sharing best practices, and coordinating incident management, reducing duplication and improving response efficiency. Capacity-building initiatives, including SEA-PAC Cyber training and IoT labelling programs, help partner nations develop robust cyber ecosystems and align standards, mitigating vulnerabilities that could impact Australia. Collectively, these initiatives provide a holistic approach, combining operational readiness, workforce development, and policy alignment to ensure that Australia and its regional partners can effectively prevent, detect, and respond to emerging cyber threats while reinforcing regional stability and economic security.

| | |
|---|---|
| **3.6.48** | Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope? |

Australia should deploy Cyber RAPID teams proactively to Pacific nations to conduct vulnerability assessments of critical systems, including hospital networks, electoral databases, and transport infrastructure. Using NIST SP 800-115 for technical testing and ASD's Essential Eight as benchmarks ensures rigorous, standardised evaluation and strengthens regional resilience.

Station ASD-certified analysts within partner nation CERTs to provide real-time threat hunting and intelligence sharing. This builds on Horizon 1's National Cyber Intel Partnership but is adapted to regional requirements, enhancing situational awareness and timely response capabilities.

Establish a Pacific Cyber Academy to train and credential local cyber responders. Certification against the ASD Cyber Skills Framework ensures consistent competencies, builds local capacity, and creates a sustainable regional talent pool capable of supporting ongoing cyber operations.

Expanding Cyber RAPID beyond its current scope provides tangible benefits for both Australia and partner nations. Proactive resilience missions prevent vulnerabilities from being exploited, protecting critical infrastructure and public services. Embedded threat intelligence nodes improve real-time situational awareness, enabling faster and coordinated responses to cyber incidents, while fostering long-term collaboration and trust. Establishing a Regional Cyber Reserve Force strengthens local workforce capability, reduces dependency on external support, and creates a sustainable, skilled regional talent pool. Together, these enhancements allow Cyber RAPID to move from a reactive support model to a proactive, capacity-building, and intelligence-driven approach. This comprehensive strategy strengthens regional cyber resilience, improves Australia's influence and partnerships in the Pacific, and aligns with broader strategic, economic, and security objectives in the Horizon 2 timeframe.

| | |
|---|---|
| **3.6.49** | 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 actively participate in the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) on Cybersecurity to influence the development of binding norms. Key focus areas include establishing protections against AI-enabled cyber attacks, such as deepfake disinformation campaigns, and advocating for small and medium enterprise (SME) protections under the Global Cybercrime Treaty, building on Horizon 1's Counter Ransomware Initiative.

Through forums like the APECTEL Cybersecurity Working Group, Australia can lead efforts in sharing intelligence on emerging malware campaigns, phishing trends, and other regional cyber threats. This strengthens collective situational awareness and proactive defense across the Asia-Pacific region.

Australia should contribute to technical standards development in ISO/IEC JTC 1/SC 27 for information security and the CEN-CENELEC-ETSI Smart Grid Coordination Group for smart grid security. This ensures that standards align with national strategic, economic, and security interests.

Participating in these forums allows Australia to influence global cybersecurity norms, standards, and best practices in line with national priorities. Engagement in the UN GGE and OEWG provides a platform to advocate for binding norms against emerging threats such as AI-enabled attacks, while ensuring SMEs are considered in international legal frameworks. Regional intelligence-sharing initiatives, particularly within APECTEL, enhance collaborative detection and mitigation of threats, improving collective resilience across the Asia-Pacific. Contributing to international standards development ensures Australia's technical, operational, and regulatory requirements are embedded in global frameworks, particularly in critical infrastructure sectors like smart grids. Together, these efforts promote interoperability, bolster trust, and strengthen national and regional security. By prioritizing these forums and issues, Australia can proactively shape the rules, norms, and technical standards needed to maintain cybersecurity leadership and resilience in Horizon 2.

| | |
|---|---|
| **3.6.50** | What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment? |

Australia should prioritise the adoption and integration of globally recognised frameworks such as the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001. These standards provide a common benchmark for security controls, risk management, and operational practices across sectors.

APRA CPS 234 should incorporate AI risk management requirements for financial sector tools, complementing the NIST AI Risk Management Framework (AI RMF) to ensure safe adoption of emerging technologies while maintaining financial system resilience.

Australia should harmonise privacy requirements with the EU GDPR, widely regarded as a gold standard, ensuring consistency for data handling, protection, and cross-border interoperability.

Through joint training, exercises, and operational coordination with neighbouring CERTs, Australia can uplift cyber maturity, enable faster regional incident response (e.g., ransomware, DDoS), and foster trust to strengthen collective cyber resilience.

Prioritising international regulatory alignment enables Australia to maintain global interoperability, facilitate cross-border collaboration, and enhance national resilience. Adopting NIST CSF and ISO/IEC 27001 ensures security practices are consistent with global best practice, reducing friction for multinational operations. Incorporating AI risk governance into APRA CPS 234 addresses emerging threats in the financial sector while aligning with international AI risk frameworks. Harmonising privacy regulations with GDPR promotes trust, legal compliance, and safe cross-border data flows. Beyond standards, regional capacity-building through training, exercises, and CERT collaboration strengthens operational preparedness, enabling faster response to incidents that impact multiple countries, such as ransomware or DDoS campaigns. By combining regulatory alignment with operational coordination, Australia can lead by example, improve regional resilience, and demonstrate strategic leadership in promoting consistent, effective cybersecurity practices across the Indo-Pacific in Horizon 2.

## Conclusion

The ISC2 Sydney Chapter's submission underscores the critical need for a cohesive and proactive national approach to cybersecurity in Horizon 2. By championing standardized frameworks, enhanced collaboration, and targeted support for vulnerable sectors, Australia can significantly strengthen its cyber resilience. The recommended actions from adopting a unified threat-sharing platform to investing in workforce development and regional partnerships are practical, scalable, and aligned with global best practices. Implementing these measures will not only address current gaps but also future-proof the nation's digital economy against evolving threats. A concerted effort across all levels of government, industry, and the community is essential to building a secure, resilient, and thriving cyber future for Australia.

## END