Cybersecurity Coalition

29 August 2025

*Submitted via homeaffairs.gov.au online submission form*

Department of Home Affairs

Government of the Commonwealth of Australia

# Submission to Horizon 2 of the Australia Cyber Security Strategy 2023-2030

**Introduction:**

The Cybersecurity Coalition (the Coalition) appreciates the opportunity to provide input on developing Horizon 2 of Australia's Cyber Security Strategy. The Coalition is composed of leading cybersecurity companies dedicated to consensus-driven policy solutions that improve cyber risk management for organizations of all sizes.

We commend the Australian Government's collaborative consultation model and its commitment to international best practices. Our responses emphasize alignment with international standards, risk-based and proportionate regulation, robust stakeholder engagement, and integration and harmonisation with existing regimes. We encourage the Government to continue its consultative approach and to promote this model internationally as a best practice for cyber policy development.

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

The Coalition observes several major trends and emerging technologies that will shape Australia's cyber threat landscape in the coming years.

First, the proliferation of Internet of Things (IoT) and connected devices will continue at pace. Australia, like other major economies, is projected to see significant growth of connected devices through 2027, expanding the attack surface available to malicious actors. Ensuring the security of these devices (for example through the baseline IoT security standards) will be critical.

Second, the increased adoption of artificial intelligence (AI) and machine learning across industries presents new cybersecurity challenges (such as AI-driven attacks or data poisoning) alongside opportunities for improved defense..

Third, the rise of quantum computing on the horizon means Australia must start preparing for a post-quantum cryptography world to protect sensitive data against future quantum decryption capabilities.

Beyond technology trends, several strategic factors should guide Horizon 2. Offence is being commoditised: RaaS, initial-access brokers and gen-AI tooling are lowering barriers for criminals and state proxies alike. More aggressive nation-states are pre-positioning in critical infrastructure and OT, and "living off the land," blurring attribution and shrinking warning time, while grey-zone campaigns blend cyber operations with influence, IP theft and economic coercion. Adversaries are also aiming at the digital backbone, cloud, identity providers, MSPs and software supply chains creating, outsized, cross-sector impacts, amid norm erosion and regulatory fragmentation that they exploit.

**2. Does the high-level Model (for monitoring cyber security outcomes) resonate, and do you have any suggestions for its refinement?**

The Coalition finds the high-level evaluation model outlined in the Discussion Paper broadly sensible as a conceptual framework for monitoring cyber security outcomes. We agree with the emphasis on measuring progress across multiple dimensions (such as cyber awareness, threat reduction, and resilience) to capture the Strategy's impact in a holistic way. The model's recognition of the dynamic threat environment, and the need to adapt metrics over time, is especially important.

We suggest a few refinements for consideration: First, the model should incorporate clear baseline metrics from the end of Horizon 1 so that improvements in Horizon 2 can be quantified. For example, establishing current benchmarks for small business cyber maturity, incident response times, or adoption rates of security standards will enable meaningful tracking of progress. Second, we recommend integrating private sector data sources (such as annual threat reports) and feedback loops into the model.

The Coalition also emphasizes that evaluation results should be transparent and shared publicly to maintain accountability. Ensuring the model captures real-world security improvements (for businesses and citizens) will be key to demonstrating Horizon 2's success.

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

The Coalition believes a multifaceted approach is needed for greater uptake of existing cybersecurity resources by SMBs and NFPs, who often lack awareness or capacity to utilize these tools. First, Government should invest in promoting and simplifying access to programs like the Small Business Cyber Resilience Service and Cyber Wardens. Many small organizations are unaware these resources exist; a targeted marketing campaign (potentially through channels like local chambers of commerce, business associations, and the ACNC for nonprofits) can raise awareness. Communications should emphasize that these services are low-cost or no-cost, practical to use, and designed for organizations with limited IT staff.

The Government might provide small grants or tax offsets for SMBs that complete certain cybersecurity training or implement recommended controls. Alternatively, establishing a voluntary "Cyber Ready SMB" badging or certification (with criteria linked to using these resources) could motivate participation, similar to how health and safety compliance is

incentivized. Customers and partners would gain confidence in businesses that have the badge, creating market pressure to participate.

Finally, leveraging intermediaries will help. Many SMBs rely on IT service providers or accountants for advice. Government can work with these trusted advisors to disseminate information about programs. Likewise, using peer ambassadors (SMB owners who have successfully improved their cyber resilience) to champion these resources in their communities can lend credibility.

By actively publicizing resources, streamlining their delivery, introducing smart incentives, and engaging community networks, the Government can significantly boost uptake of existing cyber resilience programs among SMBs and NFPs, thereby strengthening this vital segment of Australia's economy against cyber threats.

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

Many existing standards (ISO/IEC 27001, the ISM) are resource-intensive and not easily consumable by SMBs/NFPs. There is value in SMB-tailored baselines (e.g., UK Cyber Essentials; ASD Essential Eight Maturity Level One) packaged accessibly. The Government should evaluate and officially endorse one or more simplified baselines, map them to advanced standards to provide a growth path, and integrate them into procurement/grants to incentivize uptake. Provide templates/tools (risk assessment forms, policy templates) that operationalize the baseline. A recognition/badging program ("cyber safe small business") would further drive adoption.

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

Cyber insurance plays a vital role in strengthening the resilience of Australia's small and medium-sized businesses (SMBs) and not-for-profits, ensuring they can recover quickly from disruptive cyber incidents. While the cyber insurance market experienced sharp price increases during the ransomware surge of recent years, the market has since stabilized and now offers more capital and broader coverage than ever before. Given these market conditions, many in the cyber insurance market do not see product affordability as the principal barrier to uptake. Instead, the challenge lies on the demand side, driven largely by limited awareness of cyber risk, misconceptions about product relevance, and gaps in understanding the value of risk transfer. This lack of education also leaves SMB customers less likely to make investments in their cybersecurity and thus less resilient to attacks from cyber criminals.

The discussion paper rightly notes that SMBs are disproportionately vulnerable to cyber incidents and often lack the capacity to protect themselves adequately. Public statistics suggest that around 20% of Australian SMBs hold standalone cyber policies, but analysis from Cyber Coalition member companies indicates the real figure is closer to 10%. Many SMBs underestimate their exposure or believe they are not targets, despite ACSC data showing that the

average cost of cybercrime for small businesses has increased by 8% in the past year. This gap in perception likely has a direct impact on insurance adoption.

Increasing education on cyber hygiene, resilience, and risk management, including the role of insurance, should be a central pillar of the national strategy. By focusing on demand generation rather than market intervention, Australia can expand the reach of a market that already offers accessible and affordable protection for most SMBs.

**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?**

The ransomware threat remains one of the most persistent and damaging risks to the Australian economy, with Australia consistently ranking among the top ten most targeted countries globally. The government's introduction of mandatory ransomware payment reporting, along with resources such as the Ransomware Playbook, has been critical in building an evidence base and supporting victim response. However, measuring the full scope of the threat remains challenging due to underreporting, especially among small entities.

The US insurance and digital forensics and incident response sectors have observed that while payment rates have declined, a sign that prevention measures and efforts to discourage payment are having an effect, threat actors have adapted by becoming more aggressive. This includes adopting "double extortion" tactics and compressing the time between initial compromise and ransom demand. SMBs, in particular, are often targeted multiple times, and the cost of recovery can be catastrophic without robust preparation and support. The continued evolution of these criminal business models underscores the importance of intelligence sharing between government, law enforcement, insurers, and industry partners to anticipate shifts in adversary tactics.

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

The first priority in ransomware response must always be the protection of individuals, critical services, and essential business functions. Public policy should avoid penalizing victims, recognizing that ransom payment decisions are often made under significant operational or safety duress. Instead, efforts should focus on prevention, disruption of threat actors, and coordinated support for recovery, directly aligning with the objectives of Shield 1: Strong businesses and citizens and Shield 3: World-class threat sharing and blocking.

Under Shield 1, the Cyber Incident Review Board should help small and medium-sized businesses (SMBs) access expert, sector-specific recovery advice based on tactics, techniques, and procedures of current ransomware trends. Getting this information rapidly through existing ACSC infrastructure would ensure SMBs can access immediate technical, legal, and strategic guidance during an incident, reducing downtime and costs.

Under Shield 3, publishing anonymized, near-real-time intelligence from the mandatory ransomware payment reporting regime would allow SMBs, many without sophisticated

monitoring capabilities, to take timely defensive action against active threats. In parallel, expanding international disruption operations such as Operation Aquila and leveraging ASD's cyber capabilities to dismantle ransomware infrastructure and seize illicit assets would impose real costs on ransomware actors and reduce the volume of attacks reaching Australian businesses.

This dual-shield approach, combining victim-centred support with aggressive disruption and proactive intelligence sharing, would make ransomware harder to deploy, less profitable to execute, and easier for SMBs to defend against, ensuring the Australian economy is better protected across Horizon 2.

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

The regulations that most reduce cyber risk in Australia are those that are risk-based, outcome-focused, and aligned with widely adopted international standards. At the core is the Security of Critical Infrastructure (SOCI) Act, whose risk-management programs, incident notification, and enhanced obligations for Systems of National Significance drive uplift where failures would have the greatest cascading impact. The Privacy Act 1988, especially APP 11 and the Notifiable Data Breaches scheme, provides an economy-wide baseline for protecting personal information and forcing timely breach disclosure, which is crucial because almost every organisation processes personal data. The Cyber Security Act 2024 will complement these by enabling minimum security standards for consumer smart devices (lifting the security of edge devices where compromises often start), introducing mandatory ransomware payment reporting (giving visibility to disrupt the business model), establishing a Cyber Incident Review Board (to turn incidents into systemic fixes), and clarifying limited-use obligations for incident data. In finance and other high-impact sectors, APRA's CPS 234 embeds proportionate controls and board accountability, including for third-party risk, which has positive spillovers across supply chains.

Just as important are the enablers that make these regimes work better and lower net risk: harmonised incident and scam reporting across SOCI, the Privacy Act and sectoral rules; a single reporting portal; and clear safe-harbour protections for good-faith threat sharing and at-scale network blocking so defenders can act quickly without legal uncertainty.

Consistent with positions advanced by the Coalition to Reduce Cyber Risk (CR2) and the Cybersecurity Coalition, mapping obligations to consensus frameworks such as ISO/IEC 27001/27002, ISO/IEC 27110/27103, the NIST Cybersecurity Framework, and IEC 62443 for OT keeps rules interoperable and outcome-oriented, reducing compliance cost while improving real-world adoption. Where stakes and architectures differ transport, healthcare, energy OT, targeted sector guidance and rules ensure proportionate controls without defaulting to prescriptive checklists.

For Horizon 2, the priority should be to keep SOCI truly risk-based (clear thresholds, proportionate timelines, focused scope of "critical"), fully operationalise the Cyber Security Act

2024's device standards and ransomware reporting (ideally reinforced by clear, consumer-friendly security labels), finish reporting harmonisation with safe harbours to unlock scaled threat sharing and blocking, codify recognition of international standards across regulation and procurement to eliminate duplication, and sustain CPS 234's accountability model where appropriate in other systemic sectors. Together these measures drive disciplined, board-level risk management where it matters most, raise the baseline at the consumer/SME edge, enable fast, coordinated action on threats, and deliver clarity and consistency—reducing overall cyber risk without unnecessary compliance drag.

**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?**

Globally, leading jurisdictions are implementing secure-by-design standards for devices and critical systems, which Australia can learn from. The EU's Cyber Resilience Act (CRA) will cover a broad range of connected products including industrial and operational technology, mandating that manufacturers build in security and handle vulnerabilities responsibly.Australia should monitor the CRA's progress – though ambitious, it underscores that outcome-focused and appropriate criteria for device security are crucial.

For operational technology (OT) (industrial control systems, energy grid controls, etc.), international standards like the IEC 62443 series and the NIST SP 800-82 guide are widely recognized. A risk-based approach again stands out: critical sectors in the US and EU are moving toward frameworks that require OT operators to assess risks and implement controls without prescribing specific tech. For example, the EU's NIS 2 Directive sets broad security outcome requirements for operators of essential services, while allowing firms to choose the specific technical standards to meet them. Australia's own critical infrastructure risk management program (under the SOCI Act) aligns with this philosophy by mandating a risk management framework for asset owners. To strengthen OT and CER security, Australia should consider targeted standards or codes of practice (perhaps under the Cyber Security Act or sector regulations) that ensure things like network segmentation, secure remote access, and incident response plans for OT environments. These could draw on global best practices such as the U.S. electricity sector's NERC CIP standards or international guidelines from the World Economic Forum and ISA/IEC, adapted to the Australian context.

In summary, international best practice favors outcome-based standards coupled with clear baseline requirements. For edge and consumer devices, this means adopting global IoT security baselines (as the UK and others have) and possibly implementing a security labeling scheme to empower consumers.

For CER and OT systems, it means requiring adherence to proven security frameworks and not leaving legacy operational tech as a blind spot. Approaches that work best are those that leverage existing standards (rather than reinventing the wheel) and involve industry collaboration. A

voluntary baseline that can become mandatory over time could work well for CER and OT. Australia's participation in forums like the International Electrotechnical Commission (IEC) and standards harmonization efforts will ensure our frameworks for these technologies stay aligned with global norms, making implementation easier and more effective.

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

The government should continue to issue clear, principles-based guidance on emerging technologies that emphasizes security, ethics, and resilience by design. For technologies like artificial intelligence (AI), quantum computing, and advanced communications (6G), Australia can develop guidance aligned with international frameworks as they are agreed to ensure safe and responsible use. This guidance should include best practices such as conducting thorough risk assessments for new technology deployments, implementing "red team" testing to identify vulnerabilities or misuse potential, and ensuring human oversight in critical applications.

A key national security risk of AI and other emerging technologies is the potential for malicious use or unintended vulnerabilities. For example, AI models could be exploited to generate disinformation at scale or to discover zero-day vulnerabilities in software, and poorly secured systems may be hijacked by adversaries. Government guidance should therefore encourage organizations to subject AI systems to independent security evaluations, test for bias and attack vectors, and establish clear channels for experts to report vulnerabilities or safety issues without fear. Sector-specific guidelines for example, in healthcare or finance could further detail how to implement secure development lifecycles, safeguard training data integrity, strengthen resilience against adversarial inputs, and regularly audit outputs.

Another serious risk is the concentration of technology supply chains in ways that adversaries can exploit for instance, reliance on foreign-made hardware with potential backdoors, or overdependence on one or two companies for a critical technology. Guidance and policy should focus on supply chain risk management and diversification.

To support safe uptake, the government could also launch regulatory sandboxes or pilot programs for emerging technologies, where companies can innovate under supervision and share lessons about security implications. For example, a voluntary "AI security sandbox" could allow new systems to be tested in partnership with government and the research community, ensuring issues are identified early and guidance is updated accordingly.

The most serious national security risks of emerging technologies like AI include cyber and data security threats, misuse by malicious actors, and erosion of public trust if deployed without safeguards. AI, for example, can be weaponized for cyber attacks (such as automated phishing or vulnerability discovery) and influence campaigns (such as deepfakes). Government guidance should directly address these risks, advising on countermeasures such as applying AI for

defensive cybersecurity and creating verification mechanisms for digital content. It should also ensure that the legal environment encourages good-faith security research, enabling experts to responsibly test new technologies for weaknesses and disclose them safely. Extending coordinated vulnerability disclosure practices into these new technology domains will further strengthen resilience.

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

A proactive cyber security posture for Australian industry should be built around five key pillars, each of which the government is well placed to support.

First, government should provide risk-based frameworks and guidance by endorsing and harmonising internationally recognised standards such as the ISO/IEC 27000-series, the NIST Cybersecurity Framework, and sector-specific standards like APRA CPS 234. This will give industry a consistent baseline aligned with global best practice while reducing regulatory fragmentation. Clear, principles-based guidance helps businesses embed security into their operations without stifling innovation.

Second, the government can incentivize investment in resilience. Tax incentives, targeted grants, and recognition programs can encourage businesses to go beyond minimum compliance and adopt proactive practices such as implementing protective DNS, establishing vulnerability disclosure policies, and investing in continuous threat hunting. By rewarding leadership rather than only penalising failure, government signals that resilience is a competitive advantage.

Third, trusted information-sharing and joint exercises must become routine. Expanding platforms for real-time threat intelligence exchange between government and industry, and embedding regular joint incident response exercises into the National Cyber Exercise Program, will normalise cross-sector collaboration. This ensures that critical players are well-practised in working together during large-scale attacks, strengthening systemic resilience across the economy.

Fourth, safe pathways for security research and innovation are essential. Laws and regulations should explicitly enable good-faith security research and responsible vulnerability reporting, so that industry can identify and fix weaknesses before adversaries exploit them. Protecting researchers and providing clear disclosure channels will strengthen trust, improve transparency, and accelerate the remediation of systemic vulnerabilities.

Finally, government should provide practical tools for supply chain assurance. Helping organisations assess vendor security, encouraging diversification of critical technology suppliers, and maintaining clear standards for trusted products and services will reduce systemic concentration risks. As industries increasingly depend on global digital supply chains, this assurance function is critical to safeguarding Australia's sovereignty and resilience.

Taken together, these measures describe a proactive posture where industry treats cyber resilience as a core business priority, and government acts as a convener, enabler, and standard-setter. By aligning standards, rewarding investment, fostering trusted collaboration, supporting innovation, and securing supply chains, Australia can build a resilient cyber ecosystem that anticipates threats and sustains public trust.

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

The government can further support industry to block threats at scale by investing in initiatives that turn intelligence into action quickly and consistently across the economy. The National Cyber Intel Partnership (NCIP) has already demonstrated how industry collaboration canbe catalysed by Government. What is needed now is for this model to be resourced and expanded at pace, with government committing funding, technical infrastructure, and coordination support so that more sectors, especially critical infrastructure and SMEs, can benefit from collective protection.

Building on this, government should accelerate deployment of protective DNS and automated blocking services in partnership with ISPs, telcos, and service providers. By integrating intelligence from ACSC and ASD through CTIS that can be acted on automatically, malicious domains and campaigns can be blocked at scale before they cause harm. This would extend protection beyond large enterprises to cover small businesses and households that are most vulnerable.

Government should also expand trusted threat-sharing platforms such as ISACs and sector-specific networks, ensuring that information is disseminated rapidly and directly into blocking systems. At the same time, legal clarity and safe harbour protections are needed so that organisations can act decisively to block threats, whether by sinkholing domains or filtering malicious traffic, without fear of liability.

Finally, the National Cyber Exercise Program should incorporate large-scale threat-blocking scenarios, allowing industry and government to test and refine the processes, tools, and partnerships required to make blocking at scale routine without mistakes pertaining to legitimate traffic.

By resourcing NCIP to grow quickly, embedding automated protective DNS, strengthening threat-sharing pipelines, and creating the legal and operational conditions for decisive action, the government can help industry block threats at the speed and scale required to stay ahead of adversaries.

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

A thriving threat sharing ecosystem in Australia requires sustained government–industry engagement, the inclusion of smaller and less mature organisations, and strong links to international intelligence flows. Creating sovereign-only ISACs risks duplicating effort, fragmenting trust, and cutting Australian entities off from the richer global data sets needed to detect and respond to cross-border campaigns.

The more effective path is to expand Australian participation in mature international ISACs that already provide trusted frameworks, global expertise, and economies of scale. Government should focus on reducing barriers, such as awareness, cost, and access, for SMEs and low-maturity sectors so they can benefit from these communities.

The Health Cyber Sharing Network is a commendable initiative, but its long-term value will depend on how well it plugs into established international ISACs rather than operating in isolation. By resourcing access to these mature ecosystems and ensuring domestic pilots are globally connected, Australia can strengthen intelligence sharing while avoiding fragmentation and duplication.

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

Reaching whole-of-economy scale on vulnerability disclosure means making VDPs a predictable national baseline, not a boutique best practice. The fastest way to do that is to align the big policy levers so they all point the same direction. At the legal layer, enact a uniform, statutory safe-harbour for good-faith security research, harmonised across Commonwealth, state and territory law and mapped to ISO/IEC 29147 and 30111 and explicitly aligned with the EU's NIS2 directive, which requires essential and important entities to maintain vulnerability handling and coordinated vulnerability disclosure (CVD) processes supported by CSIRTs. Mirroring NIS2's expectations would give multinationals regulatory coherence and set a clear floor for Australian firms. At the market layer, use procurement to pull the supply chain: require a public VDP for all software, hardware and services procured by Commonwealth entities and government-owned corporations. Signal regulatory upside by explicitly recognising VDPs as evidence of "reasonable steps" under privacy law, as good practice inside SOCI risk-management programs, and as supportive of prudential and sectoral rules (e.g., CPS 234), so boards see risk reduction rather than red tape.

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

Yes, the balance is broadly right. Given Australia's risk profile, the combined obligations under the SOCI framework and the Cyber Security Act 2024 are proportionate so long as they continue

to be outcome-based, harmonised, and practical. To keep burden aligned with benefit, regulators should: (1) maintain a single, "report-once, use-many" approach across SOCI, privacy and sectoral rules; (2) recognise equivalency to international frameworks (ISO/NIST) to avoid duplicate audits; and (3) scale obligations by risk and size, with templates, tooling and phased timelines for SMEs.

Crucially, the enforcement posture should remain education-first, compliance assistance, guidance, and corrective action plans, shifting to penalties only for grievous failures, wilful non-compliance or repeated, material harm. Graduated responses paired with clear thresholds, safe harbours for prompt disclosure, and practical playbooks will keep the burden proportionate while still driving the uplift the Strategy seeks**.**

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

Australia should focus where our effort can set practical, widely adopted baselines. Globally: stay active in the UN OEWG (and successor process) on responsible state behaviour, the UN Cybercrime Convention, and the Counter Ransomware Initiative (CRI) for collective disruption, sanctions coordination and joint guidance. In standards-making, lean into ISO/IEC (JTC 1/SC 27) and ITU-T for security baselines (IoT, 5G/6G, software assurance), while defending the multistakeholder model through IETF, ICANN and the IGF. For economic rules, use the OECD and G20 to align risk-based approaches and metrics, and the WTO/APEC digital trade tracks to hard-wire interoperable security requirements into cross-border data and cloud. Regionally, prioritise ASEAN (ARF and ministerial cyber tracks) and the Pacific Islands Forum, and use minilaterals—Five Eyes and the Quad—to prototype norms and operational playbooks that can scale.

On issues, Australia should push: peacetime protection of critical infrastructure; interoperable incident reporting (common thresholds, timelines and formats) with reciprocal recognition; product and software security baselines and consumer labels for connected devices, aligned with leading international schemes; coordinated vulnerability disclosure mapped to ISO/IEC 29147/30111; supply-chain transparency and resilience (secure-by-design, SBOMs, vendor risk disclosure); scam/fraud–cyber fusion for cross-sector intelligence sharing and takedowns; AI and quantum security-by-design (secure model lifecycle, safety evaluations, crypto transition); and sustained capacity building and mutual assistance across Southeast Asia and the Pacific, including regional threat blocking and interoperable crisis response.

To make this bite, Australia should lead by example (PSPF, SOCI and Cyber Security Act implementations mapped to international baselines), table model clauses (portability, escrow, customer-held keys, VDP requirements) in procurement and trade, co-sponsor concrete proposals at the UN OEWG (e.g., common incident schema pilots and CBMs), and co-chair CRI working groups while running joint exercises and measurement pilots with ASEAN and Pacific partners so agreed norms translate into operational practice.

When states commit egregious cyber violations or flout agreed norms, act with allies to impose timely, proportionate, and escalating consequences: coordinated public attributions, synchronized sanctions and travel bans, joint law-enforcement and disruption operations, targeted export controls, diplomatic measures, and rapid defensive support to affected partners. Use coalitions such as Five Eyes, the Quad, and the CRI to pre-agree response playbooks and thresholds so actions are swift, lawful and collective. No one group is the answer; this lattice-work of groupings will position Australia to maximize its strengths.

Respectfully Submitted,
The Cybersecurity Coalition

29 August 2025