Consultation on Developing Horizon 2 of the 2023–2030 Australian Cyber Security Strategy

Axon Public Safety Australia Pty Ltd

29 August 2025

[redacted]

Executive Summary

Axon welcomes the opportunity to contribute to the development of Horizon 2 of the 2023–2030 Australian Cyber Security Strategy. This submission reflects Axon's practical experience supporting cyber resilience across multiple critical and essential service domains, including law enforcement, defence, health, transport, environment, mining, and local government.

Axon commends the Department of Home Affairs for its leadership in developing a world-first, long-horizon strategy that is structured, consultative, and focused on measurable outcomes. Horizon 2 builds on important foundations already in motion, including the Essential Eight maturity uplift, SOCI Act reforms, the ACSC Partnership Program, national takedown services, and the Joint Cyber Security Centres. These initiatives demonstrate the Department's capacity to both regulate and enable, and they must persist and scale. These foundations position Australia to measure progress by real outcomes—service continuity, faster detection and recovery—rather than activity counts.

Axon strongly supports the Strategy's horizon model and its shield-based structure. It provides an organising framework that is both practical and ambitious, capable of guiding Australia through accelerating technological advancement and escalating threats. For Horizon 2 to achieve lasting impact, the focus must remain on measurable uplift, proportionate regulation, and collaboration that delivers real outcomes with a clear emphasis on measurable uplift, proportional obligations, and implementation that works for both government agencies and private operators.

Australia has an opportunity to continue shaping global best practice in cyber security policy. This requires persistence in implementation, a careful balance between regulation and innovation, and a commitment to avoid frameworks that create reporting without delivering security maturity. Equally important is the need to learn from international experience, adapt proven models from trusted partners, and invest in the sovereign capabilities that will make Australia resilient in its own right.

This submission translates these principles into practical recommendations aligned to the Horizon 2 consultation questions.

Overview of Recommendations

This submission addresses selected Horizon 2 consultation questions where practical implementation detail can lift outcomes for Australian Government agencies and private businesses.

The summary table maps each recommendation to consultation questions, states the core proposal, and the intended benefit. The detailed sections then expand each item with context, a short case example, and clear outcomes.

This paper deliberately avoids restating well-established practices (e.g. awareness campaigns, baseline hygiene) or duplicating input already gathered through existing collaborations. The aim of this paper is to provide **targeted, pragmatic insights** that will help shape Horizon 2 implementation in ways that deliver real benefit to Australia.

Recommendation	Questions	Core Proposal	Intended Benefit
Outcome-focused, Maturity-tiered Framework	Q3, Q4, Q16, Q36	Evolve the outcome-based model into a tiered maturity framework - universal baseline outcomes (e.g., detect, contain, recover) for all entities, with progressive tiers for larger and critical operators. Incorporate live operational metrics alongside policy compliance	Delivers a framework that scales from SMBs to telcos and Defence; avoids shallow "tick-box" measures; ensures uplift is visible and comparable across sectors
Balance Regulation with Innovation	Q16, Q17, Q33, Q35	Design obligations that uplift cyber maturity while allowing flexibility in implementation. Build in periodic reviews to retire or refine rules that don't deliver measurable resilience gains	Keeps regulation proportionate and adaptive; reduces the risk of innovation being stifled by static or duplicative compliance
Harmonise across regulators	Q16, Q17, Q33, Q35, Q37	Progress toward "comply once, demonstrate many" by aligning outcomes and evidence across the SOCI Act & RMP Rules, Privacy Act & APP 11, APRA CPS 234 , and ASD ISM/Essential Eight. Develop a Common Controls Evidence Pack reusable across regulators.	Reduces duplication across regulators; frees scarce security talent from reporting overhead; improves clarity for both large and small operators
Operational threat intelligence	Q24, Q26, Q28, Q29	Strengthen CTIS/TISN and ACSC advisories by:	Creates a trusted, usable threat sharing ecosystem that scales across business sizes; enables

		1) embedding maturity tiers (baseline info for SMBs, richer data for critical sectors); 2) ensuring timeliness; and 3) introducing safe-harbour protections for contributors	faster integration into defences without exposing contributors to liability
Scaled proactive defence	Q24, Q25, Q26, Q27, Q30	Expand government-led takedown, disruption, and DNS blocking operations. Ensure outputs integrate with ISP and enterprise defences. Clarify national posture in peacetime vs crisis	Reduces threat volume before reaching businesses; provides predictability in conflict or crisis; strengthens resilience across all sectors
Practical OT and edge security standards	Q18, Q19, Q20, Q21, Q23, Q34	Develop pragmatic baseline standards for OT and edge devices, aligned to international best practice but locally enforceable. Include tiered expectations - baseline for smaller operators, advanced controls for critical infrastructure	Protects essential services (utilities, health, transport) without overwhelming smaller operators; builds trusted supply chains
Sovereign workforce pathways	Q39, Q40, Q41, Q42, Q43	Incentivise mid-career entrants from policing, defence, OT, and adjacent fields. Expand regional placements and university partnerships to produce cleared, industry-ready talent. Introduce mandatory cyber and online safety education across schools and universities to grow baseline awareness and spark pathways into the profession.	Builds depth and diversity in Australia's workforce; ensures government and private operators can access talent appropriate to their maturity and risk profile

Outcome-focused, Maturity-tiered Framework

Consultation Questions: Q3, Q4, Q16, Q36

Context

The Department's move toward outcome-based policy is welcome and overdue. Too often, regulation measures activity — number of audits, frequency of training, or evidence of process documentation — rather than the actual security maturity of an organisation. This risks creating a compliance culture where resources are directed toward paperwork instead of uplift.

Australia's environment is also highly diverse. Small and medium businesses need accessible pathways to demonstrate progress, while large telcos, utilities, financial institutions, and defence suppliers must be held to far higher expectations. A one-size-fits-all approach risks being either too shallow for critical operators or too burdensome for smaller entities.

Recommendation

- Require all Horizon 2 initiatives to articulate **clear, measurable outcomes**, not just activity inputs
- Embed a **tiered maturity model** that allows SMBs to demonstrate progress against simplified indicators, while requiring advanced controls from critical operators
- Use operational metrics such as patching timelines, service continuity, and incident detection times, not proxies like policy counts
- Use leading indicators (e.g., patch cadence achieved, hardening coverage) alongside lagging indicators (e.g., time to detect, time to recover) so uplift is visible during, not just after, incidents.

Case Example / Lessons from practice

Resilience exercises in Australia have shown that traditional inputs — such as the number of staff trained or policies documented — often fail to predict whether critical services remain operational during a cyber incident. The UK NCSC's Cyber Essentials Framework also emphasise outcome-based indicators over activity proxies. Horizon 2 could draw on these approaches to ensure measurement reflects capability in practice, not just compliance effort.

Intended Benefit

- Ensures regulatory effort translates into **real resilience uplift**, not just compliance artefacts
- Provides **clarity and comparability** across industries and organisation sizes
- Helps Government and industry to **prioritise investment** in the controls and practices that most directly reduce risk
- Avoids the cycle of new frameworks that impose cost without measurable benefit

Balance Regulation and Innovation

Consultation Questions: Q16, Q17, Q33, Q35

Context

Australia's regulatory landscape is becoming increasingly complex, with overlapping requirements under the SOCI Act, Privacy Act reforms, CPS 234, and multiple sector-specific frameworks. While well-intentioned, this overlap risks diverting scarce security resources toward reporting rather than genuine defence uplift. For small and medium operators in critical infrastructure supply chains, duplicative compliance can also deter participation in government contracts or slow adoption of security controls.

Recommendation

Design regulation that uplifts security maturity while minimising duplication and administrative burden. Regulatory settings should:

- Calibrate obligations by size and risk—set baseline for SMBs and higher-tier expectations for large and critical operators, with clear examples of "what good looks like" at each tier
- Ensure new obligations are evidence-based and clearly tied to uplift in resilience outcomes
- Keep flexibility so sectors can adapt controls to their context

Case Example / Lessons from practice

During the introduction of the SOCI Act enhanced obligations, several operators reported that overlapping audit and reporting requirements with APRA's CPS 234 framework created uncertainty and duplicated effort. The lesson was that harmonisation and proportionality matter as much as the control itself.

Internationally, Singapore's Cybersecurity Code of Practice provides a useful example: requirements are outcome-based, but regulators allow sector-specific tailoring and proportionality in implementation. This helps achieve uplift while giving operators space to innovate within their own contexts. The practical lesson: proportionality and reuse of credible assurance reduce drag without lowering the bar.

Intended Benefit

- Frees industry resources from administrative overhead to reinvest in frontline security
- Builds trust that regulation is targeted, proportionate, and designed to deliver outcomes rather than paperwork
- Encourages innovation and agility by allowing organisations to meet objectives in the most effective way for their context

Harmonise Across Regulators

Consultation Questions: Q16, Q17, Q33, Q35, Q37

Context

Even where regulation is proportionate, fragmentation across regulators remains a major barrier. Entities operating across sectors face a patchwork of overlapping obligations. For smaller operators in critical supply chains, the cost of meeting multiple, unaligned standards can be prohibitive. Without a common baseline, compliance becomes a resource drain and does not necessarily correlate with stronger security outcomes.

Recommendation

Progress toward a "comply once, demonstrate many" model that harmonises expectations across the SOCI Act, Privacy Act reforms, CPS 234, and sector-specific frameworks. Practical steps could include:

- Publish a cross-walk of outcome measures and control objectives across the SOCI Act/RMP Rules, Privacy Act (APP 11), APRA's CPS 234, and ISM/Essential Eight, mapped to maturity tiers
- Endorse a Common Controls Evidence Pack that regulators accept as equivalent evidence, enabling "comply once, demonstrate many times"
- Formal agreements so evidence from one trusted regulator (e.g. APRA) is accepted by others

Case Example / Lessons from practice

Multi-regulated entities frequently respond to similar evidence asks from different regulators, increasing cost without improving security signal. This fragmentation increases costs without delivering clearer national visibility of resilience.

The EU's NIS2 Directive illustrates a path toward harmonisation: it sets a common baseline across member states but allows sector regulators to build on it only where risk justifies. A similar layered approach in Australia could achieve both national uplift and sector specificity.

Intended Benefit

- Reduces duplication and compliance costs across industries
- Clarifies obligations for operators, especially SMBs and supply chain partners
- Ensures regulatory effort translates into measurable resilience rather than fragmented reporting

Operational Threat Intelligence

Consultation Questions: Q24, Q26, Q28, Q29

Context

Australia has invested in multiple mechanisms for cyber threat information sharing, including the Trusted Information Sharing Network (TISN), the Cyber Threat Intelligence Sharing (CTIS) platform, and ACSC advisories. The ecosystem is improving but uneven; outside major banks and telcos, intelligence can be too generic or slow to integrate into day-to-day defensive tooling. Without automation, intelligence stops in inboxes instead of feeding defences.

Recommendation

Evolve existing threat-sharing arrangements into a more automated, actionable ecosystem. Key steps could include:

- Expand sector-specific communities of trust within TISN, ensuring intelligence is timely, relevant, and contextualised
- Standardise on open formats (e.g. STIX/TAXII) so intelligence can flow directly into defensive technologies
- Provide safe-harbour protections to encourage faster disclosure and reduce liability fears when sharing suspected threats
- Strengthen linkages between CTIS and ACSC advisories so information reaches both large operators and SMBs in usable form

Case Example / Lessons from practice

During the Optus and Medibank incidents, industry feedback highlighted delays in getting threat intelligence that could be operationalised quickly. By contrast, in the US, the Joint Cyber Defence Collaborative (JCDC) has demonstrated the value of co-developing machine-readable indicators with industry and pushing them rapidly into defensive tools. A local adaptation — building on CTIS but with stronger automation and sector tailoring — would ensure intelligence gets from "PDF to prevention" faster.

Intended Benefits

- Moves intelligence from passive reports to real-time defensive action, improving speed and accuracy of response
- Reduces duplication by aligning CTIS, TISN, and ACSC advisories into a more coherent ecosystem
- Encourages greater industry participation in sharing by lowering legal and reputational risk through safe-harbour protections

Scaled Proactive Defence

Consultation Questions: Q24, Q25, Q26, Q27, Q30

Context

Australia has made progress in disrupting malicious infrastructure, including takedown operations coordinated by the ACSC and partnerships with telcos to block phishing and malware sites. However, the scale and speed of these efforts remain inconsistent, and many businesses and citizens still face threats that could have been neutralised upstream. At the same time, there is limited clarity on what Australia's "proactive cyber posture" should look like — in peacetime or in crisis. Without a shared baseline, industry can struggle to align its defences or know what support to expect from government.

Recommendation

Expand Australia's capacity to block and disrupt threats at scale. Clarify the national posture so industry knows what to expect. Actions could include:

- Strengthen automated DNS and IP blocking services in partnership with telcos, ISPs, and cloud providers
- Increase the visibility of takedown and disruption outcomes, giving businesses confidence that threats are being reduced "upstream"
- Define Australia's proactive cyber posture, including thresholds for action in peacetime and escalation triggers during crisis scenarios
- Run joint disruption exercises with ISPs, cloud providers, and large operators to test legal authorities, escalation thresholds, and hand-offs before a crisis

Case Example / Lessons from practice

In the UK, the National Cyber Security Centre (NCSC) Active Cyber Defence program blocks millions of malicious domains through its Protective DNS service, with measurable reductions in harm. A comparable Australian service already exists in pilot form but could be expanded and more widely integrated with industry tools. Similarly, Singapore's Cyber Security Agency has defined clear public/private roles in cyber disruption, which Australia could adapt to its federal context.

Intended Benefit

- Reduces the volume of malicious traffic reaching Australian businesses and citizens
- Provides industry with clarity on government's disruption role and expectations in different scenarios
- Reduces adversary dwell time and the volume of malicious traffic that endpoints must handle

Practical OT and edge security standards

Consultation Questions: Q18, Q19, Q20, Q21, Q23, Q34

Context

Operational technology (OT) and edge devices are increasingly networked and exposed, particularly in critical infrastructure, transport, health, and resource sectors. Vulnerabilities in these environments can lead not just to data loss but also to physical safety risks and service outages. Existing standards such as IEC 62443 and NIST's Cybersecurity Framework are valuable, but they can be resource-intensive and difficult to apply across smaller operators or highly diverse environments. Australia needs a pragmatic baseline — enforceable, internationally interoperable, and locally practical.

Recommendation

Establish national baseline standards for OT and edge devices that are outcome-focused and proportionate. This should include:

- A pragmatic "minimum controls" set aligned with IEC 62443 but simplified for Australian operators, particularly in sectors with limited security expertise
- Clear guidance on secure configuration, lifecycle management, and patchability requirements for connected devices
- Address supply-chain risk explicitly - require provenance, vulnerability disclosure pathways, and patch support commitments from OT/edge vendors

Case Example / Lessons from practice

In the US, the Cybersecurity and Infrastructure Security Agency (CISA) has published sector-specific OT security performance goals that provide operators with a prioritised, implementable set of practices. Singapore has similarly issued sector-specific guidance for smart grids and medical devices. These examples show the value of taking global standards and distilling them into practical baselines that can actually be implemented by operators of different sizes and maturities.

Intended Benefit

- Reduces systemic risks across critical services by addressing weakest-link vulnerabilities in OT and edge environments
- Provides clarity and consistency for operators, vendors, and regulators while avoiding unnecessary compliance burden
- Strengthens Australia's supply chain resilience and aligns domestic practice with trusted international partners

Sovereign Workforce Pathways

Consultation Questions: Q39, Q40, Q41, Q42, Q43

Context

Australia faces a persistent shortage of skilled cyber professionals, particularly in cleared roles supporting government, defence, and critical infrastructure. While entry-level initiatives are growing, gaps remain in mid-career pathways, regional access to opportunities, and practical education that prepares graduates for operational environments. At the same time, community-wide digital resilience starts with embedding cyber awareness and online safety from an early age.

Recommendation

Develop a sovereign cyber workforce strategy that combines education, mid-career transition pathways, and industry–academia partnerships. Key recommendations include:

- Embed mandatory cyber and online safety education across schools and universities as core digital literacy
- Incentivise mid-career entrants from adjacent fields (e.g., policing, defence, operational technology, risk management) through funded reskilling and placement programs
- Expand regional placements and pathways to broaden the talent pool beyond metropolitan centres
- Partner with universities and TAFEs to align curricula with industry needs, including pathways for security clearances and hands-on operational training
- Drive research collaboration between government, academia, and industry on applied cyber problems, ensuring efforts are coordinated and focused on national priorities

Case Example / Lessons from practice

Israel's approach to cyber education includes mandatory exposure to cyber and digital safety in schools, while Singapore's Cybersecurity Associates and Technologists program funds mid-career retraining. Both countries illustrate the benefit of coordinated, end-to-end workforce strategies that span early education through to advanced industry placements. Australia's AustCyber pilot programs and Defence Industry Pathways offer useful foundations, but scaling them nationally with a stronger focus on cleared and operationally ready roles will deliver greater impact.

Intended Benefit

- Builds a larger, more diverse, and operationally ready cyber workforce
- Reduces reliance on overseas expertise while strengthening sovereign capability
- Embeds lifelong cyber resilience by starting with education from school age
- Supports regional economic development by opening pathways outside metro hubs

Conclusion

Axon strongly supports the Department of Home Affairs' leadership in developing Horizon 2 of the 2023–2030 Cyber Security Strategy. The consultation process, the clear structure across Horizons and Shields, and the focus on measurable outcomes represent a world-first approach that can position Australia as a global leader in cyber resilience.

Our submission emphasises the need to:

- Anchor policy in outcomes that reflect real resilience gains, not reporting volume
- Balance regulation with innovation to ensure obligations drive uplift rather than overhead
- Harmonise requirements across regulators to make compliance achievable and meaningful
- Scale proactive defences and intelligence sharing in ways that integrate with industry operations
- Build practical standards for OT and edge security that protect essential services
- Invest in sovereign workforce pathways, embedding cyber literacy from early education through to cleared, mid-career roles

These recommendations are not abstract aspirations. They reflect operational lessons from Australia's public and private sectors, informed by international experience. Implemented together, they will ensure Horizon 2 delivers more than policy—it will deliver capability.

The challenge now is persistence: turning frameworks into measurable uplift, keeping obligations proportional, and ensuring Australia's approach is coordinated, pragmatic, and credible.

Axon stands ready to contribute expertise and collaborate with government and industry peers to make this ambition real.

Glossary

Term	Definition
ACSC	Australian Cyber Security Centre, the government's lead agency for operational cyber security
APRA	Australian Prudential Regulation Authority, regulator of banks, insurers, and superannuation funds
CPS 234	Prudential Standard on Information Security, issued by APRA, which sets minimum requirements for information security management
Critical Infrastructure (CI)	Systems and assets essential to the functioning of the nation, covered under the SOCI Act
ISM	Information Security Manual, published by the Australian Signals Directorate as a risk management framework for cyber security
Maturity model	A structured framework that measures the maturity of cyber security capabilities across progressive levels, from basic to advanced
NFP	Not-for-profit organisation
Outcome-based policy	Regulation or strategy that focuses on achieving measurable results (e.g., reduced breaches, faster recovery) rather than mandating specific activities
Proactive defence	Government or industry-led actions that disrupt, block, or neutralise threats at scale, rather than reacting after incidents occur
Resilience	The ability of organisations and systems to prepare for, withstand, recover from, and adapt to adverse cyber events
SMB / SME	Small and Medium-sized Business/Enterprise
SOCI Act	Security of Critical Infrastructure Act 2018 (as amended), which establishes obligations for owners and operators of critical infrastructure
Sovereign capability	Domestic capacity to design, deliver, and sustain cyber security functions without reliance on foreign providers
Threat intelligence	Information about current or emerging cyber threats, including indicators of compromise, tactics, techniques, and procedures (TTPs) used by malicious actors
TISN	Trusted Information Sharing Network, an Australian government forum for industry and government collaboration on critical infrastructure resilience

About Axon

Axon is a global technology organisation with deep operations and investment in Australia. Our Australian teams work directly with police, defence, health providers, transport authorities, councils, and other critical service operators. This breadth gives us first-hand visibility into the challenges of securing sensitive data, operational technology, and mission-critical services under multiple regulatory regimes.

The Axon Infosec Team focuses on protecting data, systems, and services relied upon by Australian partners. Axon operates within the frameworks set by Australian law, including the Security of Critical Infrastructure Act (SOCI), the Privacy Act, and sector-specific regulations.