Response to the Developing Horizon 2 of the *2023-2030 Australian Cyber Security Strategy* Policy Discussion Paper

Contents

Introduction

Fortinet welcomes the opportunity to contribute to the Horizon 2 consultation process. We acknowledge the progress made under Horizon 1 that has strengthened Australia's cyber resilience foundations. This submission responds to the discussion paper drawing from Fortinet's global threat intelligence and operational experience. We have included a series of recommendations aligned with the Government's strategic direction.

3.1 Outlook and Trends

From Fortinet's global vantage point, analysing over 100 billion events daily across more than half a million customers, three trends stand out:

- The convergence of information technology (IT), operational technology (OT), and internet of things (IoT) systems.
- The disruptive implications of AI, quantum and hyperscale adoption.
- The centrality of supply chain resilience.

The 2023–24 Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report [1]recorded 87,400 cybercrime reports, with 11% involving critical infrastructure. Credential compromise was the entry vector in nearly one-third of these incidents. The Fortinet 2025 Global Threat Landscape Report (GTLR)[2] confirms the industrialisation of attacks. Automated scanning now averages 36,000 probes per second across IT, OT, and IoT services, reflecting adversaries' ability to find vulnerable targets and exploit vulnerabilities at speed. More than 1.7 billion stolen credential records were circulating on dark markets, fuelled by credential harvesting and credential marketplaces. Ransomware operations have also consolidated, with a small number of groups responsible for a disproportionately large share of observed victims.

Fortinet's 2025 Cyberthreat Predictions Report[3] anticipates further specialisation in Cybercrime-as-a-Service, with distinct operators offering phishing, initial access, and data-exfiltration services. Quantum computing also poses future risks to cryptography, underscoring the need for an orderly transition roadmap. Against this backdrop, Horizon 1 rightly strengthened Australia's approach to data protection, but Horizon 2 must also ensure the risks of interruption to critical infrastructure services are weighted equally. These trends underscore why this next phase should support the shift to Continuous Threat Exposure Management (CTEM). By embedding machine-speed visibility, adversary emulation and risk-based remediation across government and critical infrastructure, CTEM can help align regulatory obligations with the tempo of adversary automation.

Measurement indicators should be established to provide clear benchmarks and reporting cycles for cyber uplift, including CTEM adoption rates, SOCI-sector maturity levels and workforce pipeline targets. These would enable government and industry to track progress, adapt quickly, and ensure that investment in resilience delivers measurable outcomes.

[1] Australian Cyber Security Centre (ACSC), Annual Cyber Threat Report 2023–24, https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

[2] The Fortinet 2025 Global Threat Landscape Report https://www.fortinet.com/resources/reports/threat-landscape-report

[3] The Fortinet 2025 Cyberthreat Predictions Report https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-prediction-2025.pdf

Fortinet's global threat analysis confirms the industrialisation of scanning and the rapid trade in stolen credentials, highlighting why adversary automation continues to outpace traditional compliance-driven cybersecurity.

Recommendations:

1. Support embedding of cyber-physical resilience in SOCI, CIRMP and ACSC guidance.
2. Contribute to a cryptographic transition roadmap aligned with ASD's post-quantum planning.
3. Complement AI assurance and governance initiatives by focusing both on safe adoption and adversary use.
4. Harmonise cyber security regulations and certifications to support industry implementation.
5. supply-chain assurance with EU and US comparators to maintain interoperability.
6. Encourage adoption of Continuous Threat Exposure Management (CTEM) across government and critical infrastructure.
7. Define benchmarks and reporting cycles for Horizon 2 objectives (CTEM adoption, maturity levels, workforce pipelines).

3.2 Shield 2 – Safe Technology

From Fortinet's perspective, the technology challenge in Horizon 2 is the increasing breadth and scale of threats is a symptom of the systemic conditions that allow adversaries to succeed. Insecure product lifecycles, fragmented governance in multivendor environments, and the adversarial use of emerging technologies such as AI are points where risk concentrates. They undermine trust in digital products, leave high-value datasets at risk, and complicate adoption of new technologies. Addressing them requires collaboration between government and industry, and transparency of obligations and responsibilities.

IoT and operational devices are likely to remain in service long after vendors cease to patch or support them. Vulnerability debt accumulates silently as operators continue to rely on outdated systems. Accountability must be clear on both sides. All vendors should disclose expected product lifecycles, end-of-support timelines, and patch pathways. While all operators, from government agencies, critical infrastructure providers, small to medium enterprises (SME) and not for profits (NFP), should embed this information into procurement, asset planning and disposal. Improved operator education is essential to connect vendor transparency with operator accountability.

The greater risk is procurement is not a choice between single vendor platforms versus multivendor product ecosystems, but how these digital environments are governed. Fortinet's intelligence shows breaches often occur at the seams, where controls are split and no single point of accountability exists. This Horizon can help strengthen governance obligations under SOCI so that interoperability, assurance, and clear lines of responsibility are embedded across systems.

Adversaries are already exploiting AI to generate deception, including deepfakes. The World Economic Forum's Cybersecurity Outlook 2025[4] found that two-thirds of organisations expect AI to materially impact security this year, yet only 37 percent assess AI tool security before deployment. It would be valuable for this phase of Horizon 2 to focus on embedding AI assurance requirements, including provenance checks, SBOMs for AI models and adversarial testing. Quantum computing threatens

[4] The World Economic Forum's Cybersecurity Outlook 2025, https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

cryptographic stability, requiring a national roadmap aligned with ASD and NIST. Cloud adoption is accelerating faster than compliance and skills capacity. Assurance requirements should extend consistently across IoT, edge and cloud environments and use cases.

International comparators are moving quickly. The EU Cyber Resilience Act[5] and US Secure by-Design[6] initiatives are setting international expectations. Consideration should be given to benchmarking against these to ensure interoperability and avoid duplicative compliance for Australian operators.

Obligations will only succeed if they can be implemented. Horizon 2 actions should be supported by practical playbooks and conformance tools for device security, SBOM use, and OT/IoT environments. Expanding ACSC guidance to cover OT and IoT would help entities put obligations into practice. Education-led compliance is particularly important for SMEs and NFPs, who may not have large compliance teams. Transparency of expectations and access to tools will position them to meet obligations without undue cost.

Procurement is one of government's most effective levers for secure technology adoption. It can be used to reinforce accountability and transparency, reduce duplication, and provide both government and industry with practical tools to implement obligations. Agencies are mandated to apply Foreign Ownership Control and Interference (FOCI) assessments when procuring ICT, which sets a solid baseline for supply-chain assurance. In practice, vendor responses may be treated as the FOCI assessment itself, rather than as input to a deeper, agency-led analysis. Horizon 2 can mitigate this risk by reinforcing the roles: vendors provide disclosures, while agencies retain accountability for analysis, supported by playbooks, training and spot checks.

Procurement can also be used to facilitate the adoption of Secure by Design principles and their transition into Secure by Demand in the marketplace. DTA model clauses should embed requirements such as lifecycle transparency, SBOMs, vulnerability disclosure processes and minimum configuration standards into contracts and panels. Publishing example clauses and schedules would help agencies apply these consistently and provide suppliers with clarity on expectations.

From a compliance perspective current pathways create duplication and delay. It would be valuable for this phase of Horizon 2 to focus on recognising DISP and IRAP outcomes within SOCI compliance and allow conditional acceptance where an entity is engaged in the accreditation process and a mitigation plan is in place. Aligning assurance cycles in this way would reduce burden while maintaining focus on robust outcomes. This would be particularly valuable for SMEs and NFPs, for whom repeated processes impose disproportionate costs.

Fortinet contributes to these outcomes through our global threat intelligence, by embedding SBOM practices, by extending Zero Trust across IT, OT and IoT environments, by delivering post-quantum readiness in the latest version of our core operating system (FortiOS 7.6), and through our role as one of the industry leaders in the creation of the Secure by Design pledge and as one of its earliest signatories.

[5]EU Cyber Resilience Act, NIS2 Directive https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[6] US Cyber Defense Agency, Secure by Design Pledge https://www.cisa.gov/resources-tools/resources/cisa-secure-design-pledge

Fortinet has embedded SBOM practices through the Secure by Design pledge, showing how disclosure and transparency can reduce legacy exposure when written into procurement frameworks.

For SMEs and NFPs, the challenge is less about cyber literacy and more about compliance burden. Multiple overlapping assurance cycles increase costs and delay uplift. Streamlining pathways across SOCI, DISP and IRAP would reduce duplication and ensure smaller operators are not priced out of compliance.

Recommendations

1. Mandate lifecycle transparency by requiring vendors to disclose support timelines, patch pathways and SBOMs, and requiring operators to manage these obligations in procurement and asset planning.
2. Strengthen assurance as a governance function by embedding interoperability and accountability in SOCI obligations, supported by ACSC playbooks and guidance for OT and IoT.
3. Make procurement a strategic risk tool by clarifying the role of FOCI assessments as inputs to agency-led analysis, embedding Secure by Demand clauses through DTA contracts, and aligning SOCI, DISP and IRAP obligations.
4. Incentivise vendor implementation of the transparency principle central to Secure by Design by looking during the procurement process for information that technology offerors are committed to reporting and mitigating Common Vulnerabilities and Exposures to (CVE's) in their products. Anticipate emerging technology risks by embedding AI assurance requirements and publishing a national post-quantum cryptography roadmap aligned with ASD/NIST standards.

3.3 Shield 3 – Threat Sharing and Blocking

Fortinet recognises the challenge for Home Affairs in leading the national cyber strategy across a diverse threat landscape. Nation states pursue long-term strategic objectives, while criminal actors and hackers pursue short term gains, with a relatively small number of ransomware groups causing outsized financial harm. Initial Access Brokers and markets in stolen user credentials connect these various ecosystems. Threat sharing is both a national security function and an enabler of greater productivity. This next phase provides the opportunity to ensure threat sharing reflects this diversity and that Australia can block concentrated criminal infrastructure at scale.

Fortinet recognises that intelligence sharing best creates value when it is fast, streamlined, and trusted. Incident reporting is an invaluable part of threat intelligence. Operators face overlapping obligations under SOCI, the Privacy Act and sector regulators. This creates duplication and reporting fatigue. Streamlined reporting would reduce burden and improve the quality of intelligence inputs. The Treasurer's Economic Reform Roundtable identified regulatory simplification as a national priority. A consolidated 'tell-us-once' cyber incident reporting pathway would align with that agenda, while improving the timeliness and quality of threat information for government. Horizon 2 can explore this coordination opportunity in partnership with regulators, ensuring that privacy and trust safeguards are built in.

The criminal cyber ecosystem has both chokepoints and areas of redundancy, and that focusing efforts to interdict criminal infrastructure on its bottlenecks can have an outsized impact. Ransomware operations are dominated by a relatively small number of criminal groups that rely on credential markets and Initial Access Brokers as force multipliers. This concentration makes disruption of these groups and this

infrastructure highly effective, especially when action is conducted internationally. INTERPOL's Synergia II[7] dismantled more than 22,000 malicious servers across 95 countries, while Serengeti 2.0 resulted in over 1,200 arrests and USD 97 million recovered. Fortinet is an active contributor in these disruption efforts through our partnerships with INTERPOL and other law enforcement agencies. There is an opportunity to build on these lessons by developing disruption pipelines with law enforcement, telcos, and ISPs, so that criminal infrastructure can be taken down quickly within Australia, alone or in conjunction with international partners.

The value of the Cyber Incident Review Board (CIRB) lies not only in reviewing incidents but in acting as a governance mechanism. Fortinet supports its role in connecting regulators, industry, and international partners into a single learning cycle. Embedding outputs into sector playbooks, procurement templates and APS Academy training would ensure lessons learned are applied consistently. CIRB insights can also flow securely to AFP and INTERPOL, enabling Australian experience to strengthen international disruption efforts and ensuring global lessons return to operators here.

Fortinet recognises that even with stronger intelligence and disruption, large-scale incidents will continue to occur. National readiness will require surge teams, national exercises, and cross-sector mutual aid arrangements. There is an opportunity to improve consultation and trust between government and industry clearer processes for vendor participation. Embedding these practices in ACSC and CIRB guidance would provide consistency and build confidence across sectors.

Delivering these outcomes in practice draws on Fortinet's experience through partnerships with the Cyber Threat Alliance, INTERPOL and the WEF Centre for Cybersecurity, helping translate global signals into local action. We have also supported government leading by example in areas such as Zero Trust and Secure by Design. Deploying Zero Trust and CTEM approaches across government networks would both enhance their resilience and provide exemplars and a potential roadmap for regulated industries.

Fortinet's experience with the Cyber Threat Alliance shows how intelligence can move from incident review to operational playbooks within weeks, ensuring findings do not remain abstract.

Recommendations

1. Explore a consolidated 'tell-us-once' cyber incident reporting pathway to unify SOCI, Privacy and sectoral obligations, aligned with national productivity and regulatory reform priorities, supported by privacy safeguards, automation, and standardised formats.
2. Operationalise CIRB as a governance mechanism by embedding findings into sector playbooks, procurement templates and APS Academy training, with secure pipelines to AFP and INTERPOL.
3. Strengthen blocking at scale by developing disruption pipelines with law enforcement, telcos, and ISPs, informed by international disruption operations.
4. Build national incident response capacity through surge teams, national exercises and mutual aid arrangements, embedded in ACSC and CIRB guidance.

[7] INTERPOL Synergia II, https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-cyber-operation-takes-down-22-000-malicious-IP-addresses

3.4 Shield 4 – Protected Critical Infrastructure

Horizon 1 reforms, including SOCI strengthening, CIRMP obligations and the creation of the CIRB, raised planning and reporting maturity across critical sectors. Horizon 2 is the opportunity to translate this progress into operational resilience, particularly in sectors such as advanced manufacturing, robotics, and logistics. Disruption in these areas cascades into regulated critical infrastructure and national supply chains.

ACSC reporting confirms that critical infrastructure continues to be disproportionately targeted, with credential compromise a persistent entry point. This reinforces why benchmarking uplift is essential, but we must move beyond compliance inputs to measure resilience in outcomes: fewer successful intrusions, faster recovery, and defined maturity levels across OT and IoT. Fortinet's 2025 OT and Cybersecurity Report[8] strengthens this point, showing that half of OT organisations experienced an incident in the past year, yet those with integrated governance under a CISO or CSO had 65% fewer intrusions and faster recovery. Transparent reporting against such indicators would demonstrate whether reforms are delivering resilience in practice.

Operators consistently tell us that resilience uplift must reduce duplication rather than add new layers of compliance. SOCI and CIRMP already impose significant requirements, and adjacent sectors such as advanced manufacturing and logistics often lack the resources to successfully navigate multiple overlapping frameworks. Fortinet's experience across both regulated and unregulated sectors shows that outcome-based benchmarks, consolidated assurance pathways and alignment with international standards can ease this burden.

Horizon 2 can strengthen this role by embedding outputs in sector playbooks, procurement guidance and APS Academy training. CIRB insights can also flow into joint disruption operations with AFP and INTERPOL, linking national incident review to international disruption activity.

Many Australian operators are embedded in global supply chains. Interoperability with EU and US frameworks would reduce duplicative reporting and allow firms to better focus on strengthening assurance. There is potential to map SOCI and CIRMP obligations to these standards and explore mutual recognition. OT and IoT testbeds and joint resilience exercises would provide the venue to test guidance, validate CIRB playbooks and align operational standards with trusted partners.

Fortinet can support in delivering these outcomes drawing on experience in securing OT and critical environments, including mapping platforms to IEC-62443 standards, ruggedising systems for industrial contexts and monitoring OT and ICS exploits through FortiGuard Labs.

Fortinet sees Horizon 2 as the stage to embed maturity benchmarks and recovery targets directly into CIRMP guidance, supported by ACSC advisories and sector-specific testbeds to trial practical responses.

[8] Fortinet 2025 State of Operational Technology and Cybersecurity, https://www.fortinet.com/resources/reports/state-ot-cybersecurity

Recommendations

1. Embed outcomes-based maturity uplift into CIRMP and ACSC guidance, with indicators covering incident reduction, recovery times and sector resilience.
2. Strengthen CIRB's role as a governance mechanism by embedding outputs into playbooks, procurement guidance and APS Academy training, and by linking insights to domestic and international disruption efforts.
3. Extend guidance and CIRB playbooks to OT and IoT environments and adjacent non-SOCI sectors such as advanced manufacturing and logistics.
4. Prioritise international alignment by mapping SOCI and CIRMP obligations against EU and US CISA frameworks, pursuing mutual recognition, and supporting OT and IoT testbeds and joint resilience exercises.

3.5 Shield 5 – Sovereign Capabilities

Sovereign capability is central to national resilience. Horizon 1 signalled this priority through SOCI reforms and early workforce initiatives. Horizon 2 is the opportunity to define sovereign capability in practice: a skilled domestic workforce, resilient SMEs, trusted innovation, and governance settings that enable secure growth while maintaining international interoperability.

It is about ensuring Australian institutions, industries and supply chains are resilient and globally trusted. Multinationals are part of this solution when they work with governments and local industries to create partnerships, localise training and standards, and embed lessons from global operations. By aligning with national investment priorities, Fortinet supports sovereign capability in ways that complement domestic industry and maintains interoperability with trusted partners.

Workforce sovereignty is the foundation of sovereign capability. The Fortinet 2025 Cloud Security Report[9] found skills and compliance gaps remain the leading barrier to secure adoption. Horizon 2 is the opportunity to build measurable workforce pipelines across the APS, graduates, and reskilled professionals. Fortinet's training and certification programs, already adopted by Australian universities and TAFEs, show how international models can align with APS Academy initiatives to accelerate capability development.

Sovereign capability also depends on digital literacy across the public sector and particularly among decision-makers. This Horizon can embed cyber resilience into APS professional development for policy, procurement, and program leaders. Building this baseline capability at the executive level ensures cyber is integrated into strategy, budgets, and governance. Fortinet's experience embedding literacy at senior levels in large organisations shows uplift is most effective when decision-makers understand cyber as a core risk and productivity issue.

CPA Australia's Essential cybersecurity insights for small business[10] shows many SMEs remain complacent, treating cyber as an IT cost rather than a business priority. Awareness-raising alone is insufficient. The strategy can now move from awareness to integrated education, embedding cyber into SME risk and

[9] Fortinet 2025 Cloud Security Report, https://www.securenetworkhub.com/sites/securenetworkhub/files/2025-Cloud-Security-Report-Fortinet.pdf

[10] CPA Australia, Essential cybersecurity insights for small business, https://www.cpaaustralia.com.au/tools-and-resources/podcasts/business-strategies/essential-cybersecurity-insights-for-small-business

productivity management training. This applies equally to business leaders, who need to see resilience as a strategic investment rather than as compliance overhead. Fortinet's experience with SME-focused training and intelligence-sharing partnerships illustrates how uplift can be delivered at scale and cost-effectively.

Innovation sovereignty requires connecting research to practice. Horizon 2 highlights PQC, OT and AI as priorities. National testbeds and pilot programs can accelerate commercialisation and reduce risk for adopters. Fortinet brings lessons from global PQC pilots, OT standards mapping and AI assurance that could be applied through NRF and Future Made in Australia programs. State centres such as South Australia's Cyber Collaboration Centre provide venues where objectives can be tested.

Procurement settings also shape sovereign capability. Embedding cyber resilience criteria into NRF, Future Made in Australia and sector programs ensures government investment supports building secure capability.

Horizon 2 is an opportunity to develop a national "compliance compass" to harmonise obligations among overlapping frameworks (SOCI, CIRMP, DISP, IRAP, Privacy). By mapping overlaps and sequencing requirements, it would reduce duplication, lower compliance costs and provide clarity for operators.

Fortinet's role in the creation of Secure by Design the Cyber Threat Alliance created to promote threat intelligence sharing between competing firms, and in IEC-62443 standards offer insights into how harmonisation can support domestic industry and promote international interoperability.

Sovereign capability means measurable workforce pipelines, resilient SMEs, secure innovation, and governance that enables industry growth without duplication. Metrics for workforce, SME participation and testbed outcomes would give government and industry visibility of progress. Strengthening sovereign capability also positions Australia as a trusted partner in the Indo-Pacific, contributing to regional resilience and security. Fortinet's SME-focused modules demonstrate how basic hygiene can be delivered without excessive cost.

Fortinet's post-quantum pilots, OT testbeds and AI assurance programs show how advanced solutions can be tested through trials and proofs of concept before committing to scaling-up deployment. Embedding similar models into NRF and Future Made in Australia programs would reduce adoption risk and accelerate commercialisation of sovereign capability.

Recommendations

1. Align proven training and certification models with APS Academy and tertiary/vocational pathways to expand sovereign workforce pipelines, with measurable targets.
2. Extend SME-focused resilience programs through intelligence-sharing and integrated education modules, embedding cyber uplift as a productivity priority.
3. Support sovereign testbeds and pilots in PQC, OT and AI, leveraging global lessons and embedding them in NRF and Future Made in Australia programs.
4. Develop a national "compliance compass" to harmonise SOCI, CIRMP, DISP, IRAP and Privacy obligations, informed by international standards and Secure by Design practices.
5. Incorporate cyber resilience criteria into government procurement and investment programs to ensure sovereign capability is secure by design.

3.6 Shield 6 – Global Leadership

Fortinet sees Shield 6 as the bridge between Australia's domestic reforms and its global leadership role. It is the space where Australia can project credibility internationally, and where trusted industry partners can help translate national lessons into global standards, disruption efforts and regional capacity building.

International comparators demonstrate useful models: the EU Cyber Resilience Act embedding secure-by-design obligations; the US Joint Cyber Defense Collaborative integrating government and industry in real time; the UK NCSC Industry100 embedding experts into national defence; and Singapore's Cybersecurity Act linking licensing to reporting and cooperation. Horizon 2 can ensure Australia draws on these lessons while projecting its own distinctive strengths.

Australia has an opportunity to shape international standards through ISO/IEC, ETSI and ITU. Insights from SOCI, CIRMP and CIRB can inform global approaches that balance security with resilience while reducing fragmentation for operators. Fortinet contributes directly to this agenda: as a Secure by Design signatory, we embed coordinated vulnerability disclosure and SBOM practices across our product development lifecycle; through the Cyber Threat Alliance we share intelligence on exploitation patterns that feed into ISO/IEC and ETSI deliberations; and as a member of FIRST, we help operationalise formats such as STIX/TAXII that promote incident response standards across borders. These experiences show how private sector data and practice can anchor government or quasi-government standards in private sector-driven operational experience.

Collective disruption is a clear lever for global leadership. Successful outcomes have been possible because pipelines between industry and law enforcement were operationalised. Fortinet has contributed to these operations by providing telemetry on command-and-control infrastructure and malware families, demonstrating how private sector intelligence can scale takedown campaigns. This next phase could adapt this model by enabling CIRB and ACSC outputs to flow into disruption pipelines with AFP and INTERPOL.

Australia has credibility in multilateral settings, including the UN Open-Ended Working Group and ASEAN digital dialogues. Horizon 2 is the opportunity to bring practical lessons from SOCI and CIRB into these forums, ensuring that emerging norms of responsible state behaviour reflect the operational realities of defending critical infrastructure. Fortinet's global intelligence work on state-linked activity provides insight into attacker behaviours and techniques, which can ground Australia's contributions in evidence rather than abstraction.

The Indo-Pacific is where Australia's credibility is most visible, and we can use this point in the strategy to embed cyber resilience into DFAT strategies, Quad initiatives, and ASEAN digital economy work. Capacity-building programs should extend to education, workforce development and technical assistance, building on mechanisms such as the Pacific Cyber Security Operational Network (PaCSON). Fortinet's Training Institute exemplifies scalable skills development through its globally recognised Network Security Expert (NSE) Certification Program, which is delivered via academic partners and authorised training centres across ASEAN and ANZ. These programs offer instructor-led and self-paced courses, hands-on labs, and certification pathways from foundational to expert levels. Fortinet's collaboration with groups like the Australian Women in Security Network (AWSN) and its Education Outreach Program further supports inclusive access for women, underrepresented communities, and economically challenged groups. This demonstrates how sovereign and regional cyber capability can be built with equity at its core.

Horizon 2 positions Australia as a trusted contributor to Western frameworks and as a bridge in the Indo-Pacific. By aligning domestic practice with international standards, linking CIRB outputs to disruption pipelines, and embedding cyber into diplomacy and development, Australia can lead through credibility. Fortinet recognises industry's role in this agenda: contributing technical insights to standards bodies, supporting global disruption operations, and delivering regional training and workforce programs that reinforce Australia's reputation as a partner of choice.

Recommendations

1. Align with leading international frameworks to ensure interoperability and shared resilience.
2. Expand Indo-Pacific capacity-building by embedding cyber workforce, education, and technical assistance in DFAT, Quad and ASEAN initiatives, supported by PaCSON.
3. Formalise industry–government pipelines into disruption operations, connecting CIRB outputs and Australian experience to INTERPOL and AFP actions.
4. Leverage SOCI and CIRB lessons, supported by industry intelligence, to shape international standards and norms through ISO/IEC, ETSI, ITU and UN forums.
5. Review industry advisory and steering groups to best capitalise on the local and global expertise in the Australian Cyber community.

Conclusion

Horizon 2 is a critical opportunity to consolidate frameworks, reduce complexity for operators, and ensure compliance translates into real resilience. It also positions Australia to lead in the Indo-Pacific while staying interoperable with global partners. Fortinet supports the Shield-based approach and stands ready to contribute expertise, data, and practical experience. Adaptive, regularly reviewed policy settings will be essential to keep pace with adversaries and emerging technologies.

Summary of Recommendations

Shield	Recommendations
3.1 Outlook and Trends	1. Support embedding of cyber-physical resilience in SOCI, CIRMP and ACSC guidance. 2. Contribute to a cryptographic transition roadmap aligned with ASD's post-quantum planning. 3. Complement AI assurance and governance initiatives by focusing both on safe adoption and adversary use. 4. Harmonise cyber security regulations and certifications to support industry implementation. 5. supply-chain assurance with EU and US comparators to maintain interoperability. 6. Encourage adoption of Continuous Threat Exposure Management (CTEM) across government and critical infrastructure. 7. Define benchmarks and reporting cycles for Horizon 2 objectives (CTEM adoption, maturity levels, workforce pipelines).
3.2 Safe Technology	1. Mandate lifecycle transparency by requiring vendors to disclose support timelines, patch pathways and SBOMs, and requiring operators to manage these obligations in procurement and asset planning. 2. Strengthen assurance as a governance function by embedding interoperability and accountability in SOCI obligations, supported by ACSC playbooks and guidance for OT and IoT. 3. Make procurement a strategic risk tool by clarifying the role of FOCI assessments as inputs to agency-led analysis, embedding Secure by Demand clauses through DTA contracts, and aligning SOCI, DISP and IRAP obligations. 4. Incentivise vendor implementation of the transparency principle central to Secure by Design by looking during the procurement process for information that technology offerors are committed to reporting and mitigating Common Vulnerabilities and Exposures to (CVE's) in their products. Anticipate emerging technology risks by embedding AI assurance requirements and publishing a national post-quantum cryptography roadmap aligned with ASD/NIST standards.
3.3 Threat Sharing and Blocking	1. Explore a consolidated 'tell-us-once' cyber incident reporting pathway to unify SOCI, Privacy and sectoral obligations, aligned with national productivity and regulatory reform priorities, supported by privacy safeguards, automation, and standardised formats. 2. Operationalise CIRB as a governance mechanism by embedding findings into sector playbooks, procurement templates and APS Academy training, with secure pipelines to AFP and INTERPOL. 3. Strengthen blocking at scale by developing disruption pipelines with law enforcement, telcos, and ISPs, informed by international disruption operations. 4. Build national incident response capacity through surge teams, national exercises and mutual aid arrangements, embedded in ACSC and CIRB guidance.
3.4 Protected CI	1. Embed outcomes-based maturity uplift into CIRMP and ACSC guidance, with indicators covering incident reduction, recovery times and sector resilience. 2. Strengthen CIRB's role as a governance mechanism by embedding outputs into playbooks, procurement guidance and APS Academy training, and by linking insights to domestic and international disruption efforts. 3. Extend guidance and CIRB playbooks to OT and IoT environments and adjacent non-SOCI sectors such as advanced manufacturing and logistics. 4. Prioritise international alignment by mapping SOCI and CIRMP obligations against EU and US CISA frameworks, pursuing mutual recognition, and supporting OT and IoT testbeds and joint resilience exercises.

3.5 Sovereign Capabilities	1. Align proven training and certification models with APS Academy and tertiary/vocational pathways to expand sovereign workforce pipelines, with measurable targets. 2. Extend SME-focused resilience programs through intelligence-sharing and integrated education modules, embedding cyber uplift as a productivity priority. 3. Support sovereign testbeds and pilots in PQC, OT and AI, leveraging global lessons and embedding them in NRF and Future Made in Australia programs. 4. Develop a national "compliance compass" to harmonise SOCI, CIRMP, DISP, IRAP and Privacy obligations, informed by international standards and Secure by Design practices. 5. Incorporate cyber resilience criteria into government procurement and investment programs to ensure sovereign capability is secure by design.
3.6 Global Leadership	1. Align with leading international frameworks to ensure interoperability and shared resilience. 2. Expand Indo-Pacific capacity-building by embedding cyber workforce, education, and technical assistance in DFAT, Quad and ASEAN initiatives, supported by PaCSON. 3. Formalise industry–government pipelines into disruption operations, connecting CIRB outputs and Australian experience to INTERPOL and AFP actions. 4. Leverage SOCI and CIRB lessons, supported by industry intelligence, to shape international standards and norms through ISO/IEC, ETSI, ITU and UN forums. 5. Review industry advisory and steering groups to best capitalise on the local and global expertise in the Australian Cyber community.