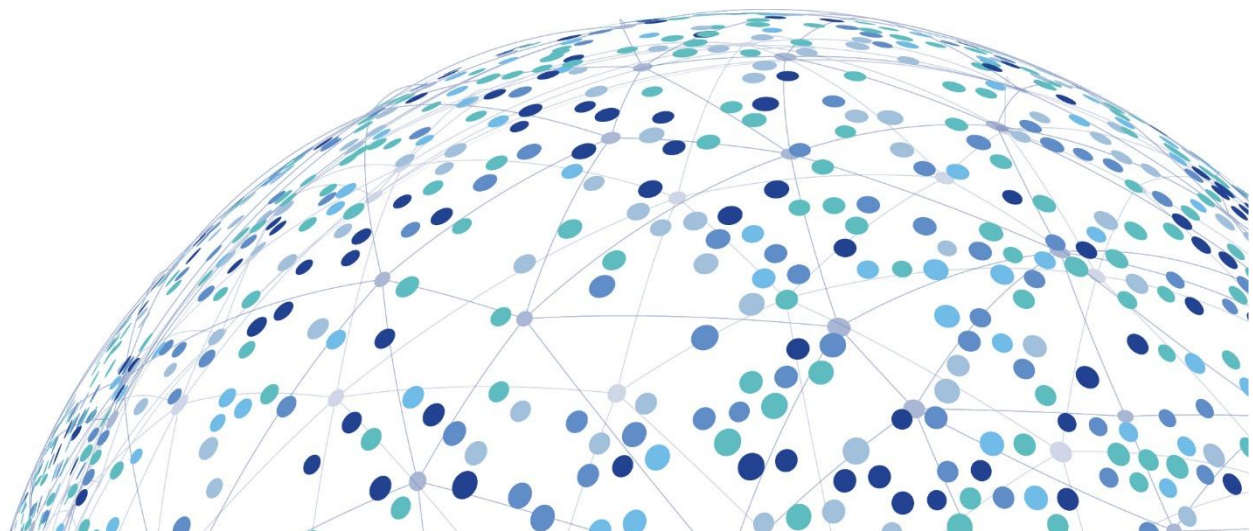
AUSCERT

AUSCERT SUBMISSION

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



Contents

Executive summary 2

What success looks like by 2028 2

About AUSCERT and methodology 2

Vision and evaluation model 4

Shield 1: strong businesses and citizens 5

Shield 2: safe technology 6

Shield 3: world-class threat sharing and blocking 7

Shield 4: protected critical infrastructure 8

Shield 5: sovereign capabilities 9

Shield 6: strong region and global leadership 10

Cross-cutting themes 11

Offers to co-design and pilot 11

Conclusion 11

Executive summary

AUSCERT welcomes the opportunity to contribute to the consultation process to develop Horizon 2 of the 2023–2030 Australian Cyber Security Strategy.

AUSCERT has sought feedback from our member organisations and staff. Through this process, we aimed to ensure small and medium businesses, who make up the majority of our membership, have a strong voice in shaping Horizon 2. The transition to Horizon 2 should focus on practical uplift at scale, especially for small and not-for-profit organisations, while strengthening national capabilities that block, share and fix threats quickly. Our community's input points to six priority areas:

1. **Scale what works for small organisations**
   Cost and capacity remain the primary barriers to adopting essential controls. Members strongly favour subsidised assessments and a simple, free baseline standard with a companion checklist.
2. **Prioritise secure by design standards for edge and operational technology**
   All domains need attention, with a clear tilt towards edge and Internet of Things, and operational technology, followed by AI-enabled products and cloud services.
3. **Stand up a national threat-blocking feed**
   There is strong support for an opt-in, government-backed blocking service that distributes high-quality, product-mapped indicators with explicit guidance on how to block.
4. **Adopt a national vulnerability disclosure programme**
   Members support a coordinated approach that provides safe harbour for researchers, clarity of scope and proportionate remediation timelines.
5. **Keep SOCI proportionate, focus on joint exercises and practical support**
   The current settings are broadly seen as directionally right, with calls for more joint exercising, reusable templates and targeted grants where risk and impact justify it.
6. **Invest in workforce pathways that convert quickly**
   Preferred levers include stackable micro-credentials, paid internships and mid-career conversion programmes, complemented by targeted skilled migration where needed. Priority sovereign capabilities include AI and OT security, domestic threat intelligence, and data-sovereign cloud and email security options.

What success looks like by 2028

- Small organisations adopt and sustain essential controls with less effort and cost, enabling their business.
- Threats are blocked at scale and earlier in the kill chain, with faster coordinated disclosure and remediation.
- Critical infrastructure operators, together with their key suppliers, exercise regularly and implement improvements, with targeted support that raises supply chain security baselines.
- Workforce pathways convert quickly into capable practitioners across priority roles.
- Regional partnerships accelerate alerting and response, and regulatory duplication reduces.

About AUSCERT and methodology

AUSCERT is a national, not-for-profit, member-based Computer Emergency Response Team (CERT)

based at The University of Queensland. As the oldest and trusted cyber security organisation in Australia, we have supported Australian organisations for over three decades with incident coordination, threat intelligence, security advisories and community enablement.

This submission is informed by feedback sought from AUSCERT staff and from representatives across our member organisations spanning education, energy, government, professional services and small business. Responses were de-identified and synthesised to identify common priorities and practical recommendations.

For further information, we are available at:
[redacted]

Vision and evaluation model

Context in brief

Horizon 2 aims to scale maturity across the economy by focusing on practical interventions with measurable outcomes. A concise, shared evaluation model will help Government and industry see what is working and adjust course quickly.

Recommendations

1. Adopt an outcome-focused logic that links inputs, outputs and outcomes.
    - *Inputs*: baseline adoption by SMEs, scaled threat blocking and coordinated vulnerability disclosure, workforce pathways and role aligned micro-credentials.
    - *Outputs*: baseline checklist completions and remediation plans issued, enforced blocks through common controls, disclosures received and coordinated, completions of recognised credentials and placements.
    - *Outcomes*: fewer material incidents, faster containment of significant events, improved resilience (e.g., response and recovery) in SMEs and critical sectors.
2. Publish a short public dashboard twice yearly, with definitions and a simple data dictionary, and provide an API for trusted partners.
3. Harmonise incident reporting thresholds and core fields across schemes to reduce burden and increase analytic value, using a core schema that sectors can extend where necessary.
4. Establish a privacy by design protocol for sharing deidentified operational data for evaluation, with appropriate governance and legal safe harbour.

Measurement

- Adoption and sustained use of the baseline checklist and associated remediation plans.
- Time from validated indicator to enforced block across common controls.
- Time from vulnerability report to remediation for participants in the disclosure programme.
- Participation in recognised workforce pathways and conversion into priority roles.
- Sector level trends in material incidents and containment times.

Data sources and cadence

Use existing reporting held by ACSC and ASD, sector ISACs and CERTs, de-identified insurer and regulator data where appropriate, and selected case studies. Report at least twice per year, with a short narrative on what has changed and why.

Shield 1: strong businesses and citizens

Context in brief

Small and not-for-profit organisations remain disproportionately exposed to common threats due to cost, capability and complexity constraints.

Recommendations

1. Publish a two-page baseline with a companion checklist that maps to common control frameworks such as the Essential Eight, with simple language and clear order of operations.
2. Fund timeboxed, subsidised assessments for SMEs, triaged by sector risk and data sensitivity, coupled with a light touch remediation plan.
3. Incentivise suppliers to ship secure-by-default configurations for small customers, supported by a simple conformance label and sample hardening guides.
4. Expand identity crime victim support, including a single triage entry point and faster credential recovery pathways.
5. Favour a collaboration-based, rather than a compliance-based approach to SME cybersecurity uplift.
6. Generally, create more funding opportunities targeted to the uplift of cybersecurity for SMEs.

Implementation supports

- Templates for baseline adoption and remediation plans.
- A supplier conformance label with clear minimums, for example MFA, logging, default encryption.
- A shared advice line for SMEs that consolidates guidance from government and CERTs.

Measurement

- Baseline checklist adoption and remediation completion rates.
- Time to contain common incidents and ransomware claim prevalence among SMEs.
- Uptake of secure-by-default supplier configurations.

Shield 2: safe technology

Context in brief

Edge and Internet of Things, and operational technology environments, present expanding attack surfaces. Cloud and AI-enabled products require clear, implementable baselines and contract terms.

Recommendations

1. Establish secure-by-design baselines for edge and OT first, followed by AI-enabled products and cloud services, with proportionate requirements for small adopters.
2. Publish a simple foreign ownership, control or influence assessment guide that is consistent across sectors and sized for SMEs.
3. Provide a practical vendor risk toolkit with risk criteria, example questionnaires and automated scoring where appropriate.
4. Encourage use of software bills of materials (SBOM) where proportionate, and include model clauses for data residency, logging and breach notice in government and public procurement.

Implementation supports

- Reference architectures and migration paths for legacy OT.
- A registry of non-conforming products and known issues to inform procurement.
- Model terms for AI and cloud procurement that reduce ambiguity for small buyers.

Measurement

- Percentage of procurements that meet secure-by-default baselines.
- Reduction in repeatable misconfigurations visible in incident reports.
- Uptake of SBOM and model clauses in contracts.

Shield 3: world-class threat sharing and blocking

Context in brief

Faster movement from intelligence to enforceable blocks, and safer vulnerability reporting, will reduce harm at population scale.

Recommendations

1. Pilot a national, opt-in blocking service that combines government, CERT and major platform signals as trusted and transparent providers, distributed through common controls such as DNS, email and endpoint.
2. Publish product-mapped advisories that state the blocking action, not only the indicator, and prioritise high-impact indicators for accelerated handling.
3. Establish a national vulnerability disclosure programme with safe harbour, a simple intake process, coordinated timelines and a public directory of participating organisations.
4. Mature sector information-sharing bodies where needed, and better align scams intelligence with cyber threat sharing.

Implementation supports

- A single technical integration guide for receiving and enforcing the national feed.
- Open formats and automation patterns for indicator handling and revocation.
- A disclosure policy template and legal-safe wording for participating organisations.

Measurement

- Coverage of the blocking feed across sectors and controls.
- Median time from indicator receipt to enforcement, and from report to remediation in disclosure cases.
- Volume and usefulness of shared advisories and joint alerts.

Shield 4: protected critical infrastructure

Context in brief

Operators are implementing SOCI obligations. Proportionality and clarity remain important, particularly for smaller operators and upstream suppliers.

Recommendations

1. Maintain proportionality while simplifying guidance and templates, especially for smaller operators and suppliers.
2. Run regular mixed-sector exercises that include managed service providers and upstream suppliers, with published improvement items.
3. Provide targeted grants where public risk and potential impact justify investment, linked to measurable uplift.
4. Align government security requirements where practicable to reduce duplication and provide a single navigation point for obligations.

Implementation supports

- Reusable templates and director-level briefings for governance and risk decisions.
- Exercise playbooks and evaluation rubrics that drive concrete improvements.
- A central navigation page that maps obligations and guidance.

Measurement

- Exercise participation and completion of after-action items.
- Time to restore essential services in exercises and incidents.
- Evidence of reduced duplication across overlapping schemes.

Shield 5: sovereign capabilities

Context in brief

Australia needs workforce pathways that convert quickly, alongside targeted development of capabilities that reduce concentrated foreign dependency.

Recommendations

1. Fund stackable micro-credentials tied to specific roles, for example analyst, incident coordinator and OT defender, and recognise them in government recruitment.
2. Co-fund paid internships and mid-career conversion or returnship programmes with industry, prioritising critical sectors and regions.
3. Support Australian threat intelligence exchange, analytics and automation capabilities that integrate with global standards.
4. Invest in OT security testing ranges and reference architectures that small operators can adopt.
5. Use targeted skilled migration to address acute shortages that cannot be met in the short term.
6. Support Australian start-ups in the sector

Implementation supports

- A national catalogue of recognised micro-credentials mapped to roles.
- Models for structured workplace learning and supervision in internships.
- Grants for domestic tooling that solves Australian use cases and can be exported.

Measurement

- Completions of recognised micro-credentials and conversion to roles.
- Internship placements and retention.
- Adoption and export of domestic tooling.

Shield 6: strong region and global leadership

Context in brief

Australia can accelerate collective resilience by deepening joint intelligence, response and supply chain security with neighbours, while aligning frameworks internationally.

Recommendations

1. Scale joint intelligence and response exercises with South-East Asia and the Pacific, including supplier ecosystems.
2. Align to practical, widely adopted frameworks such as ISO, NIST and CIS Controls, while engaging with ENISA and standards bodies to harmonise where possible.
3. Expand regional programmes that build local capacity in CERT operations, disclosure and blocking.
4. Use attributions, advisories and sanctions in a coordinated way, informed by shared intelligence and legal thresholds.

Implementation supports

- Shared playbooks and translation-ready advisories for regional partners.
- Fellowship and secondment programmes between CERTs and government.
- Joint supplier assurance initiatives for critical technologies.

Measurement

- Number of joint exercises and shared advisories.
- Time to cross-border alerting and action.
- Adoption of harmonised controls across participating countries.

Cross-cutting themes

- Harmonisation and simplicity. Reduce duplicated effort across regulatory schemes and guidance, provide single navigation points, and use consistent language and thresholds.
- Data for decision making and visibility. Link interventions to clear outcomes and publish short, regular progress updates that show what is working.
- Supplier leverage. Use procurement and conformance labels to raise the security floor for products and services used by SMEs.
- Inclusion and equity. Ensure supports reach regional and remote communities and under-resourced sectors.

Offers to co-design and pilot

AUSCERT stands ready to co-design and, where appropriate, host or coordinate pilots in partnership with government and industry.

- Facilitation of sector-specific projects aimed at strengthening existing threat intelligence frameworks, and creating new ones where required, with a view to promote threat sharing through appropriate incentives.
- Design of a national vulnerability disclosure programme, including safe harbour framing and a directory of participating organisations.
- A baseline plus subsidised assessment package for SMEs and NFPs, with simple remediation roadmaps.
- Joint exercise design that includes managed service providers and upstream suppliers.

Conclusion

Horizon 2 is an opportunity to scale measures that reduce harm in visible ways. By combining a simple baseline for SMEs, a national approach to blocking and disclosure, proportionate regulation for critical infrastructure and workforce pathways that convert quickly, Australia can lift resilience where it matters most.

AUSCERT welcomes the opportunity to continue collaborating with Government on codesigning sector-specific measures to ensure organisations can fulfil their dual role as both resilient operators and national capability builders. Thank you for the opportunity to provide feedback on Horizon 2.

For further information, we are available at:
[redacted]