Cyberstronomy Submission to Horizon 2 Consultation - Australian Cyber Security Strategy 2023–2030

1. Executive Summary

Cyberstronomy welcomes the opportunity to respond to the Horizon 2 Discussion Paper. While the Horizon 2 framework reflects commendable ambition, we believe Australia will continue to suffer serious systemic cyber failures unless bold, unambiguous reforms are enacted. In our view, the most urgent priority is the introduction of legislated, auditable baseline cybersecurity standards for all entities operating in the digital economy, tiered by revenue, and backed by clear incentives and enforcement mechanisms.

The QANTAS cyber incident, among others, underscores that voluntary compliance, aspirational awareness campaigns, and fragmented regulatory oversight are not sufficient. Without structural change, Australia's exposure to cyber risk will deepen.

2. Legislative Reform for Baseline Standards

We support the intent behind many Horizon 2 initiatives - particularly those related to SMBs, critical infrastructure, and threat sharing - but the Strategy must move beyond incentives and guidance. Cyber resilience cannot rely on goodwill or voluntary adherence to best practices.

Recommendation:
Legislate mandatory baseline cybersecurity controls, tailored to enterprise size and sectoral risk profile:

Tier	Entity Type	Example Controls
1	<$3 million turnover	MFA, patching, backups, basic endpoint protection
2	$3–50 million turnover	Tier 1 + incident response plan, staff training
3	>$50 million turnover or critical	Tiers 1–2 + threat hunting, regular audits, ISO/Essential 8 Level 2+ alignment

These controls should be auditable through self-assessment for Tier 1, accredited third parties for Tier 2, and mandatory external audits for Tier 3.

Rationale:
A tiered model ensures proportionality and avoids burdening small organisations while still driving national uplift. It mirrors successful models in the financial services and healthcare sectors internationally.

The 100 Point Cyber Check: An Accessible Tool for Tier 1 Entities

To simplify adoption for Tier 1 businesses and not-for-profits, the **100 Point Cyber Check**[1] - developed by Cyberstronomy - offers a lightweight, practical tool that:

- Aligns with Tier 1 requirements;
- Translates technical controls into plain English actions;

[1] https://www.100pointcybercheck.com/

- Generates a completion certificate for business use (e.g. for insurance or grant eligibility); and
- Provides a stepping stone toward higher compliance tiers.

This check functions analogously to the "100 point identity check" in finance and employment: a familiar concept adapted to cybersecurity readiness.

Example categories from the 100 Point Cyber Check:

- Uses Multi-Factor Authentication on key accounts (30 points)
- Applies software updates within 7 days (20 points)
- Maintains regular cloud or offline backups (20 points)
- Uses strong, unique passwords or a password manager (10 points)
- Has designated responsibility for IT or cyber matters (10 points)
- Implements free antivirus or endpoint protection software (10 points)

Score ≥ 100: Meets Tier 1 baseline cybersecurity standards

By incorporating tools like this into the regulatory framework, Australia can **balance uplift with usability**, especially for vulnerable or under-resourced organisations. There are many similar tools or risk assessment methods which can substantially reduce cyber risk in combination with a controls framework.

3. Streamlining the Cyber Regulatory Landscape

As noted in the Discussion Paper (p.17), Australia's cyber regulatory environment is currently overlapping and confusing, with obligations arising from the SOCI Act, Privacy Act, CPS 234, and multiple other instruments. This disincentivises compliance and makes it difficult for businesses to prioritise security investments.

Recommendation:

Establish a single regulatory architecture under a national Cyber Security Authority empowered to administer and harmonise cyber regulations, much like ASIC's role in financial regulation.

This should include:

- A single reporting portal for all incidents (as commenced)
- Consolidated, sector-specific guidance
- Alignment with international frameworks (e.g. NIST CSF, ISO 27001)

4. Support for Small and Medium Enterprises (SMEs)

We strongly support the Horizon 2 emphasis on cyber uplift for SMBs. However, education alone is insufficient. Many SMEs lack time, budget, and in-house expertise to meaningfully act on guidance.

Recommendation:

- Subsidised audit programs and pre-packaged toolkits tied to the tiered standards (see above)
- Integration of basic cyber hygiene checks into tax reporting or ABN renewals to drive uptake
- Encourage insurers to align cyber insurance eligibility with certified compliance levels

5. National Uplift through Enforcement and Accountability

The QANTAS cyber incident shows that even large enterprises may underinvest in cyber security when it is treated as a reputational or PR risk rather than a regulated operational risk.

Recommendation:

- Introduce a "Cyber Duty of Care" as part of director obligations under the Corporations Act
- Require mandatory public disclosure of baseline control compliance for listed companies
- Leverage the Cyber Incident Review Board powers (from the Cyber Security Act 2024) to issue sector-specific findings and enforceable undertakings

6. Strengthen Feedback Loops

We support the development of the Cyber Security Policy Evaluation Model, but urge stronger private-sector data integration.

Recommendation:

- Establish a national anonymous cyber incident clearinghouse (like VERIS/DBIR in the US)
- Allow service providers (MSPs, ISPs) to report threat telemetry trends
- Require large entities to submit de-identified metrics on control implementation and incident outcomes

7. Closing Remarks

Cyberstronomy commends the Department of Home Affairs on its continued leadership. But unless the Strategy transitions from guidance to obligation, and from aspiration to accountability, Australia will not meaningfully reduce its exposure to cyber harm.

The time for consultation is now - but the time for mandatory, proportionate, and auditable action is now too.

We are pleased to attach proposed model legislation to achieve the desired outcomes.

Sincerely,

[redacted]

[redacted] Cyberstronomy Pty Ltd
Email: [redacted] | Phone: [redacted]

Cybersecurity Baseline Standards Act 2025 (Proposed)
An Act to provide for uniform, auditable baseline cybersecurity obligations across the Australian economy, and for related purposes

Part 1 - Preliminary

1. Short Title

This Act may be cited as the *Cybersecurity Baseline Standards Act 2025*.

2. Commencement

This Act commences on 1 July 2026.

3. Objects of the Act

The objects of this Act are to:
(a) reduce systemic cyber risk across the Australian economy;
(b) establish enforceable cybersecurity obligations based on entity size and risk exposure;
(c) harmonise the regulatory landscape to improve compliance and reduce duplication;
(d) improve cyber resilience through auditable and transparent security controls.

4. Definitions

In this Act, unless the contrary intention appears:

- **Baseline Standards** means the minimum cybersecurity controls established under this Act.
- **Cyber Regulator** means the authority designated under section 6.
- **Entity** includes a corporation, partnership, trust, not-for-profit, or sole trader carrying on business in Australia.
- **Tier 1 Entity** means an entity with annual turnover below $3 million.
- **Tier 2 Entity** means an entity with annual turnover between $3 million and $50 million.
- **Tier 3 Entity** means an entity with annual turnover above $50 million or designated as critical infrastructure.
- **Designated Auditor** means a person or body accredited by the Cyber Regulator to conduct cybersecurity audits under this Act.

Part 2 - Cybersecurity Baseline Obligations

5. Application of Baseline Standards

(1) Entities must implement and maintain cybersecurity controls in accordance with the Baseline Standards for their designated Tier.
(2) The Standards apply to all entities operating in Australia, including not-for-profits and foreign corporations with a digital presence.

6. Establishment of Cyber Regulator

(1) The Minister must, by legislative instrument, designate an existing Commonwealth agency as the Cyber Regulator.
(2) The Cyber Regulator is responsible for:
(a) developing and maintaining the Baseline Standards;
(b) accrediting auditors;
(c) monitoring and enforcing compliance; and
(d) publishing annual reports on compliance and sectoral maturity.

7. Tiered Standards

(1) The Cyber Regulator must, by legislative instrument, publish and periodically review the Baseline Standards, which must include:

- For **Tier 1**: controls for multi-factor authentication, patching, backups, and basic endpoint protection;
- For **Tier 2**: Tier 1 controls plus incident response planning, access control, and staff training;
- For **Tier 3**: Tier 2 controls plus penetration testing, threat detection, vulnerability management, and external auditing.

(2) The Regulator may, by legislative instrument, prescribe additional requirements for specific sectors or high-risk activities.

8. Certification and Auditing

(1) A Tier 2 or Tier 3 Entity must:

(a) obtain an audit of its compliance with applicable Standards every 2 years; and

(b) submit the audit report to the Cyber Regulator.

(2) A Tier 1 Entity must complete a self-assessment declaration annually.

(3) The Cyber Regulator may conduct or require additional audits at its discretion.

Part 3 - Enforcement and Penalties

9. Compliance Notices and Directions

(1) The Cyber Regulator may issue a written compliance notice if satisfied an entity has breached this Act.

(2) A compliance notice may require the entity to:

(a) implement specified controls within a defined timeframe;

(b) submit to a compliance audit;

(c) cease operations until compliance is achieved (Tier 3 only).

10. Civil Penalties

(1) A Tier 2 or Tier 3 Entity that fails to comply with section 8 or a compliance notice is liable to a civil penalty of up to:

- 500 penalty units for Tier 2;
- 5,000 penalty units for Tier 3.

(2) The Federal Court may order additional remedies including injunctions, enforceable undertakings, or appointment of an external cybersecurity monitor.

11. Whistleblower Protections

Persons who report non-compliance in good faith are protected under the *Public Interest Disclosure Act 2013* and must not be subject to retaliation.

Part 4 - Miscellaneous

12. Interaction with Other Laws

Nothing in this Act limits the operation of:

(a) the *Security of Critical Infrastructure Act 2018*;

(b) the *Privacy Act 1988*;

(c) the *Corporations Act 2001*;

(d) any other law of the Commonwealth, a State or a Territory relating to cybersecurity.

13. Review of the Act
The Minister must cause a review of the operation of this Act to be conducted and tabled in Parliament within 3 years of commencement.