Introduction

The Tech Council of Australia (TCA), representing over 170 of the nation's leading technology companies, welcomes the opportunity to respond to the Government's Horizon 2 Policy Discussion Paper.

We commend the Government's ambition to make Australia a world leader in cyber security by 2030. The Council shares the conviction that cyber resilience is not only a defensive necessity but also a driver of productivity, growth, and competitive advantage. When businesses, communities, and governments can trust their digital systems, they innovate faster, adopt new tools with confidence, and compete more effectively in global markets.

Within the Council, the National Security Tech Alliance (NSTA) provides a forum for firms at the cutting edge of sovereign capability, supply-chain security, and AUKUS Pillar 2 engagement. The Alliance ensures that the perspectives of the national security technology sector are integrated into broader resilience and productivity objectives.

Overarching Themes

1. Cyber resilience is a productivity driver. Horizon 2 should explicitly frame cyber not just as protection but as a foundation for efficiency and growth. Resilience reduces downtime, lowers compliance and insurance costs, and creates the trusted environment required for digital adoption and innovation.

2. Double-down on whole-of-economy and global alignment. Horizon 1 built the scaffolding. Horizon 2 must deliver measurable uplift that strengthens productivity across the economy by:
    - harmonising regulatory obligations and working towards international cyber security regulatory alignment,
    - embedding clear, fit-for-purpose standards for SMEs and NFPs, and
    - ensuring government, industry, and citizens have aligned incentives to invest in resilience.

3. Sovereign capability should be framed as both a national security imperative and a source of competitive differentiation in global markets where trusted supply chains and transparent standards are increasingly valued.

4. Focus on alliance alignment and regional influence. Horizon 2 should ensure Australia is an indispensable partner in allied and regional settings, particularly through AUKUS Pillar 2. This not only improves security but also opens new global markets for Australian firms offering resilient, trustworthy technology.

5. Emerging Technology is the next frontier. Australia must prepare now for technologies that will redefine the cyber landscape, including:

    - Quantum encryption and quantum-safe cryptography to counter “harvest now, decrypt later” risks,
    - Artificial intelligence (AI) assurance and governance to ensure safe, trusted AI adoption,
    - 6G and advanced communications security,
    - Trusted space systems (satellites, PNT, comms), and
    - Next-generation secure cloud and edge computing.

6. These technologies present both risks and opportunities. Horizon 2 must ensure Australia is not simply reactive but is a first-mover in trusted adoption, turning national security imperatives into productivity gains and global market advantages.

Shield-Specific Response

Shield 1: Strong Businesses and Citizens

- A fit-for-purpose SME cyber standard would reduce barriers and boost productivity by cutting the time, cost, and uncertainty of compliance.

- Awareness campaigns should be measured against practical productivity outcomes (e.g. fewer incidents, faster recovery times).

- Expansion of cyber wardens and trusted-partner programs can free SMEs to focus on growth rather than recovery from preventable incidents.

Shield 2: Safe Technology

- Securing edge devices, consumer energy resources, and operational technologies ensures digital infrastructure underpins reliability and efficiency, not fragility.

- A transparent FOCI (foreign ownership, control or influence) process would streamline due diligence, saving firms time and reducing the cost of uncertainty while protecting national interests.

- Internationally aligned technical standards create efficiency gains for exporters, ensuring Australian products are “secure by design” and competitive in global markets.

Shield 3: Threat Sharing and Blocking

- Expanding ISACs and NCIP pilots will reduce duplication of effort across sectors, enabling firms to access threat intelligence once and apply it broadly.

- Clear guidance on Active Cyber Defence should include a government-led approach, with clearly defined boundaries for private sector organisations. This should explicitly prohibit private sector 'hack-back' activities.
- Joint cyber exercises should expand to include joint resilience exercises, reflecting the broader shift from cyber security to cyber resilience.
  TCA supports a voluntary approach to Coordinated Vulnerability Disclosure (CVD), aligned with international standards (pending views of other members).

Shield 4: Critical Infrastructure

- Streamlined compliance across SOCI, Privacy, and CPS 234 would free operators to invest more in uplift and less in administration.

- Sector-specific maturity pathways would allow operators to focus resources where they deliver the largest productivity gains.

There is a significant opportunity for digital government modernisation to drive both improved security outcomes and productivity gains. Legacy IT systems and the slow pace of transformation remain barriers — accelerating modernisation would benefit both government and industry.

- Addressing cross-border dependencies (cloud, cables, satellites) ensures continuity of services that underpin national productivity.

Shield 5: Sovereign Capabilities

- Workforce initiatives should target labour market productivity — easing bottlenecks, promoting diversity, and reducing the wage premium created by global scarcity.

- A National Security Tech Investment Facility could de-risk sovereign R&D, accelerate commercialisation, and open export channels.

- AUKUS Pillar 2 should be leveraged not only for capability acceleration but also for market access, enabling Australian firms to scale faster in trusted frameworks.

- Emerging technologies must be treated as a distinct cyber security priority — ensuring Australia has both the workforce and the industrial base to adopt and export secure solutions in quantum, AI, space, 6G, and secure cloud.

Shield 6: Strong Region and Global Leadership

- Positioning Australia as a cyber-resilient nation enhances its attractiveness as an investment destination.

- Regional capacity-building aligned with SEA-PAC and AUKUS ensures partners adopt secure, interoperable systems, reducing collective risk and creating larger trusted markets for Australian firms.
  Australia should also build on its leadership role to drive global cyber deterrence, ensuring

adversaries face credible costs for malicious cyber activity. This would reinforce Australia's reputation as a trusted, resilient, and secure partner.

Recommendations

1. Embed Supply-Chain Resilience as a Source of Competitive Differentiation

   Make supply-chain resilience an explicit Horizon 2 objective, spanning software, hardware, data, and critical technology inputs. Beyond mitigating risk, this should be framed as a source of productivity and competitive advantage — lowering compliance costs, reducing downtime, and positioning Australian firms as trusted providers in global markets.

2. Draw on the Success of the TISN to Build a 'Cyber State-of-Play Portal'

   Building on the Trusted Information Sharing Network (TISN), develop an accessible and simple cyber state-of-play portal that:

   - helps individuals, SMEs, and larger entities understand the threat landscape in real time,
   - shows which Strategy initiatives are designed to address which threats,
   - leverages the expertise of ASD and the Executive Cyber Council (ECC) members,
   - is compatible with any future threat-sharing programs,
   - incorporates lessons from successful models such as ISAC pilots and the Counter Ransomware Initiative/Taskforce, and
   - supports the Department of Home Affairs' intent to embed data on outcomes into the assessment of long-term effectiveness.

   This portal would provide a living state-of-play picture of Australia's cyber environment — clear, user-friendly, and credible. It would connect threats to responses and show progress over time, helping businesses make productivity-enhancing investments in resilience while giving Government and industry a shared evidence base for decision-making.

3. Harmonise and Internationally Align Regulation

   Pursue regulatory harmonisation under Horizon 2 with international alignment (OECD, Quad, AUKUS). This will cut duplicative compliance, reduce transaction costs, and create a clear, competitive environment that supports secure growth.

4. Anticipate and Integrate Emerging Technologies

   Ensure Horizon 2 is equipped to account for the rapid emergence of transformative technologies, including:

   - Quantum encryption and quantum-safe cryptography,
   - Artificial intelligence assurance and governance,
   - 6G and advanced communications security,

    - Trusted space systems, and
    - Next-generation secure cloud and edge computing.

5. These technologies are already reshaping the cyber threat landscape and the global economy. Treating them as a distinct focus under Horizon 2 would reinforce resilience, ensure policy keeps pace, and position Australia as a first-mover in trusted adoption — turning national security risk into a competitive differentiator.

Conclusion

The Tech Council of Australia and the National Security Tech Alliance strongly support the Government's Horizon 2 ambitions.

Cyber resilience is not only about protection; it is about unlocking productivity. A secure, trusted digital environment reduces economic drag, accelerates innovation, and creates competitive advantage for Australia in global markets.

We also acknowledge and endorse the Department of Home Affairs' commitment to embed data on outcomes into the assessment of long-term effectiveness. The Council sees the proposed Cyber State-of-Play Portal as the natural vehicle to deliver this vision — providing citizens, SMEs, industry, and Government with a trusted, shared picture of threats, responses, and progress.

Finally, resilience must be future-facing. Australia's competitiveness will increasingly depend on our ability to integrate and secure emerging technologies such as quantum encryption, AI, 6G, trusted space systems, and secure cloud. Embedding resilience into these technologies today will secure our sovereignty tomorrow and create a premium for Australian innovation in global markets.

By embedding resilience as a driver of growth — through supply-chain security, sovereign capability, alliance alignment, and trusted adoption of emerging technologies — Horizon 2 can secure Australia's digital frontiers while laying the foundations for a more productive, competitive, and secure economy.