SUBMISSION ON THE CONSULTATION TO DEVELOP HORIZON 2 OF THE 2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY

novera

EXECUTIVE SUMMARY

Novera believes that Australia stands at a critical juncture in its cybersecurity journey. Horizon 2 of the 2023–2030 Cyber Security Strategy represents an opportunity to move beyond piecemeal initiatives and embed the structures, standards, and safeguards that will define our national resilience for the coming years and decades.

Novera's submission identifies six pillars that we contend demand urgent and sustained attention:

1. **Artificial Intelligence and Emerging Technology Governance**: AI is a double-edged sword. It will accelerate productivity but also turbo-charge cybercrime, disinformation, and fraud. Australia must adopt and shape international frameworks to ensure transparency, safety by design, and resilience against malicious use.
2. **Digital Sovereignty and Foreign Dependency**: Australia's reliance on a handful of foreign technology multinationals is a systemic risk. Hyper-scale cloud, software supply chains, and cybersecurity platforms are too concentrated offshore. The government must implement a public register of critical vendors, require FOCI (foreign ownership, control, and influence) risk assessments, and address the disproportionate lobbying influence of foreign-owned technology firms and their peak bodies.
3. **Lifting SMBs and NFPs Beyond Awareness**: Awareness is not enough. Usability is the barrier that prevents lasting change. We recommend a consolidated ACSC portal with plain-language guidance, sector-specific templates, and self-assessment tools. Subsidised health checks delivered by AS/ISO/IEC 17024-accredited professionals and SMB capability hubs will translate policy into measurable uplift across the economy.
4. **Regulatory Reform and Harmonisation**: Australia does not need more fragmented obligations; it needs coherent, risk-based regulation. CPS 234 should be the benchmark. SOCI must be clarified and tailored to maturity levels. Privacy Act reforms must be enacted in full to include stronger safeguards, data minimisation, AI controls, and a direct right of action. Above all, obligations must be harmonised across regimes to reduce compliance fatigue and allow organisations to focus on genuine outcomes.
5. **Professionalisation of the Cyber Workforce**: Cybersecurity is not yet a profession, and it must be. The government should establish a recognition framework with protected titles, endorse AS/ISO/IEC 17024-accredited certifications, and maintain a national register of accredited practitioners. Bridging programs and stackable micro-credentials will diversify pathways, while SMB capability hubs will expand reach. This will give businesses and consumers confidence in the competence and accountability of individuals holding themselves out to be professionals operating in the sector.
6. **Global and Regional Leadership**: Australia must not be a policy taker. We should champion mechanisms such as the UN Convention on Cybercrime, lead in AI governance at international institutions such as ISO, OECD, and UN, and advocate for interoperable standards. Regionally, we must deepen ties with ASEAN, the Quad, APEC, and the Pacific, focusing on shared CSIRTs, subsea cable resilience, ransomware disruption, and common toolkits. A digital services tax, advanced through OECD/G20 forums, would ensure that global technology firms contribute fairly to our ecosystem and fund sovereign innovation.

Horizon 2 is the chance to scale national cyber maturity, strengthen sovereign capability, and embed Australia as a credible global leader. Novera's recommendations are clear: professionalise the workforce, harmonise regulation, address digital sovereignty, govern AI responsibly, and lead internationally.

Australia's resilience will not be built by awareness campaigns, fragmented standards, or reliance on foreign goodwill. This approach has been tried and to date has not yielded the right results. Novera contends that it will only be built by decisive action, professional competence, and sovereign control.

TABLE OF CONTENTS

QUESTION 1

WHAT TRENDS OR TECHNOLOGY DEVELOPMENTS WILL SHAPE THE OUTLOOK OVER THE NEXT FEW YEARS, AND WHAT OTHER STRATEGIC FACTORS SHOULD THE GOVERNMENT BE EXPLORING FOR CYBERSECURITY UNDER HORIZON 2?

Novera contends that key trends shaping the outlook include the rapid deployment of Artificial Intelligence (AI) systems, an ever-increasing dependence on foreign-controlled digital infrastructure, and the integration of operational technology (OT) and IoT in critical sectors.

Novera believes that the accelerating pace of digital transformation, without commensurate uplift in governance, will continue to elevate systemic risks across the economy, particularly as AI technologies continue to improve and be leveraged by threat actors who will use that technology for nefarious and criminal purposes.

In our view, several critical trends and developments will shape the outlook over the next five years, each carrying strategic implications for Australia's national resilience.

1. **Artificial Intelligence (AI) Deployment**: The rapid and widespread adoption of AI systems will deliver efficiency and productivity benefits, but also create systemic risk. Threat actors are already leveraging AI to automate and scale malicious activity, including phishing, ransomware, disinformation, and deepfakes. Without corresponding uplift in governance and security practices, AI will be an accelerant for cybercrime.

2. **Digital Sovereignty Risks**: Australia's increasing reliance on foreign-owned and controlled digital infrastructure, particularly hyper-scale cloud, AI, and cybersecurity service providers, raises questions of sovereignty, resilience, and economic security. In a world that is becoming increasingly protectionist, Novera contends that a strategic dependency on a small number of multinational operators concentrates sovereignty risk and reduces national control over critical functions.

3. **Operational Technology (OT) and IoT Convergence**: The growing integration of OT and IoT into critical infrastructure sectors, including energy, transport, and water, introduces new attack surfaces. These systems often operate with legacy components not designed for cybersecurity, compounding the challenge of ensuring safety, availability, and integrity.

4. **Pace of Digital Transformation**: Australia continues to digitise rapidly, but governance, regulation, and workforce capability are not keeping pace. This mismatch between transformation and governance will continue to elevate systemic risk unless addressed through Horizon 2.

OUR RECOMMENDATIONS

To address these challenges, Novera recommends the Federal Government:

1. **Advance AI Governance:** Promote and adopt AI governance frameworks aligned with international standards such as ISO/IEC 42001 and the NIST AI Risk Management Framework.
2. **Address Digital Sovereignty Risk**: Assess and mitigate risks associated with foreign ownership and control of hyperscale cloud, AI, and cybersecurity vendors and service providers.
3. **Introduce a Digital Services Tax**: Require foreign technology firms to contribute proportionately and fairly to Australia's digital and cyber resilience. Revenue raised should be allocated to funding local technology startups with a genuine Australian workforce and revenue presence.
4. **Support Local R&D and Innovation**: Establish targeted research and development grants to build sovereign capability and expand the pool of Australian-based and domiciled technology and services providers.
5. **Strengthen International Cooperation**: Advocate for and support the UN Convention on Cybercrime as the successor to the Budapest Convention on Cybercrime and facilitate the enhancement of cross-border enforcement, attribution, and cooperation on shared threats.
6. **Promote International Standards**: Encourage the adoption of security frameworks such as ISO/IEC 27001 across industry sectors, particularly small and medium enterprises, to harmonise requirements, reduce compliance burdens, and uplift national cyber maturity.

LINK TO HORIZON 2 GOALS

Novera's recommendations align with the Horizon 2 goals of scaling cyber maturity across the whole economy, expanding investment in the broader cyber ecosystem, and strengthening sovereign capability. Embedding AI governance, addressing digital sovereignty, and supporting local innovation ensures that Australia is not just resilient, but actively shaping its digital future.

QUESTION 7

HOW CAN GOVERNMENT ENCOURAGE SMBS AND NFPS TO UPTAKE EXISTING CYBER RESOURCES (I.E. SMALL BUSINESS CYBER RESILIENCE SERVICE, CYBER WARDENS, ACNC GUIDANCE ETC.)?

Novera contends that while awareness of government-provided cyber resources has improved in recent years, practical usability remains a key barrier to adoption by small and medium businesses (SMBs) and not-for-profits (NFPs).

Novera posits that many of these organisations operate with limited budgets, little to no dedicated cybersecurity staff, and are often overwhelmed by the volume and complexity of advice. Resources are frequently fragmented across multiple agencies and websites, written in technical language, or presented without clear implementation pathways.

As a result, Novera believes that many SMBs and NFPs remain vulnerable despite the existence of quality government initiatives. Addressing these barriers is critical to achieving Horizon 2's objectives of lifting baseline cyber maturity and embedding resilience across the economy.

OUR RECOMMENDATIONS

Novera recommends the Federal Government:

1. **Consolidate all resources into a single, accessible digital portal hosted by the Australian Cyber Security Centre (ACSC)**, incorporating real-world case studies, maturity self-assessments, and practical implementation checklists.
2. **Fund cyber health checks and uplift services delivered by AS/ISO/IEC 17024 certified cybersecurity professionals** operating under a recognised Australian professional certification and accreditation regime, ensuring quality and consistency of advice.
3. **Partner with Australian industry associations and chambers of commerce** to deliver localised outreach and build trust with SMBs and NFPs at the community level.
4. **Ensure materials are standards-aligned yet written in plain language**, with direct applicability to common SMB and NFP scenarios, thereby reducing barriers to practical adoption.

QUESTION 9

WHAT EXISTING OR DEVELOPING CYBERSECURITY STANDARDS COULD BE USED TO ASSIST CYBER UPLIFT FOR SMB'S AND NFP'S?

Novera forms the view that SMBs and NFPs are critical sectors in Australia's economy and society, but they often operate with limited cybersecurity resources, budgets, and expertise. In many cases, SMBs and NFPs lack dedicated security staff, budgets for certification, or the ability to interpret highly technical standards into their day-to-day context.

While Novera agrees that industry-accepted standards provide an essential foundation for cyber uplift, we argue that for small and medium businesses (SMBs) and not-for-profits (NFPs), the primary challenge is not that they do now know which standard to use; rather, it is a lack of having the practical means and capacity to implement them that is the most compelling problem which needs solving.

While Novera supports, advocates for and sees value in recognised standards such as ISO/IEC 27001, the ASD Essential Eight, the NIST Cybersecurity Framework v2.0, and standards such as ISO/IEC 42001 for AI governance are all valuable, their impact will be limited unless accompanied by accessible support structures, which Novera believes is where the Government should focus its efforts on.

For this reason, Novera contends that the Government's focus under Horizon 2 should be on making standards usable, affordable, and actionable rather than simply encouraging their adoption.

RECOMMENDATIONS

Novera recommends that functional approaches to help solve this challenge include the following:

1. **Sector-specific guidance**: Tailored advice for high-risk verticals such as healthcare, aged care, and community services, recognising differing obligations and operating realities.
2. **Practical templates and toolkits**: Plain-language policies, checklists, and self-assessment tools mapped to the standards such as the ASD Essential Eight , enabling resource-constrained organisations to act without extensive external consulting.
3. **A pool of accredited professionals who can assist**: Novera contends that Government should promote ANSI/ISO 17024-accredited or equivalent individuals, accredited by an Australian certifying body to provide trusted implementation support and assurance, avoiding inconsistent or unqualified advice.
4. **Subsidise or co-fund cyber health checks and uplift programs:** lowering the cost and effort barrier for SMB's and NFP's and encourage participation of Australian owned, operated, domiciled and tax-paying providers at scale.

LINK TO HORIZON 2 GOALS

Novera believes that anchoring SMB and NFP uplift programs to globally recognised standards while providing practical, localised support directly advances Horizon 2's objectives of scaling cyber maturity, investing in the cyber ecosystem, and growing a skilled workforce. Ensuring standards are actionable and affordable enables systemic uplift and reduces national risk exposure.

QUESTION 16

WHICH REGULATIONS DO YOU CONSIDER MOST IMPORTANT IN REDUCING OVERALL CYBER RISK IN AUSTRALIA?

Novera considers that regulation is one of the strongest levers available to the Government to reduce systemic cyber risk across the economy.

Novera notes that several frameworks already provide solid foundations. Still, they must be reinforced, expanded, and harmonised to address emerging challenges such as AI misuse, excessive data retention, and foreign dependency. Importantly, Novera considers that regulatory requirements must be streamlined to avoid unnecessary duplication, administrative burden, and compliance fatigue, particularly for small and medium enterprises and operators of critical infrastructure.

Novera contends that regulatory priorities include:

1. APRA CPS 234: CPS 234 sets the benchmark for risk-based cybersecurity regulation in Australia. Novera contends that its focus on board-level accountability and proportionate, risk-driven controls should serve as a model for regulatory uplift across other sectors, not just financial services.

2. Security of Critical Infrastructure (SOCI) Act: The SOCI Act is critical to safeguarding Australia's critical infrastructure. However, further work is required to ensure obligations are implemented in a manner that is clear, proportionate, and does not create unnecessary compliance burden, particularly for smaller operators. Harmonisation with other regulatory instruments, such as APRA CPS 234 and broader Privacy Act obligations, would significantly reduce duplication.

3. Privacy Act Reforms: Novera steadfastly believes that reforming the Privacy Act remains essential to ensuring Australia's data protection regime is fit for purpose in a digital economy, and where the ever-encroaching presence of technology into individuals' private lives requires proportionate and appropriate regulation. Novera urges the Government to continue to enact all recommendations of the Privacy Act Review in full, including:

- Stronger safeguards for sensitive and high-risk data, including health and biometric data.
- Explicit obligations addressing AI misuse and automated decision-making.
- Tighter data retention and destruction requirements to reduce risks of legacy data breaches.
- Harmonisation with global privacy regimes of our key trading partners, such as the European Union, China, Japan, India, the Republic of Korea, the United States and New Zealand
- Alignment of these reforms with SOCI and CPS 234 obligations to reduce regulatory complexity and ensure that organisations can focus on improving outcomes rather than managing overlapping compliance regimes.

RECOMMENDATIONS

Novera recommends that functional approaches to help solve this challenge include the following:

1. **Sector-specific guidance**: Tailored advice for high-risk verticals such as healthcare, aged care, and community services, recognising differing obligations and operating realities.
2. **Practical templates and toolkits**: Plain-language policies, checklists, and self-assessment tools mapped to the standards such as the ASD Essential Eight , enabling resource-constrained organisations to act without extensive external consulting.
3. **A pool of accredited professionals who can assist**: Novera contends that Government should promote ANSI/ISO 17024-accredited or equivalent individuals, accredited by an Australian certifying body to provide trusted implementation support and assurance, avoiding inconsistent or unqualified advice.
4. **Subsidise or co-fund cyber health checks and uplift programs:** lowering the cost and effort barrier for SMB's and NFP's and encourage participation of Australian owned, operated, domiciled and tax-paying providers at scale.

LINK TO HORIZON 2 GOALS

These regulatory priorities align directly with the Horizon 2 objectives of lifting national cyber maturity, strengthening sovereign capability, and building international partnerships. By enacting reforms that clarify accountability, modernise privacy law, protect critical infrastructure, and ensure a professional cyber workforce — while harmonising requirements across frameworks — the Government can materially reduce systemic risk without imposing unnecessary complexity or compliance burden.

QUESTION 20

WHAT ADDITIONAL GUIDANCE DO YOU OR YOUR ORGANISATION NEED TO MANAGE FOREIGN OWNERSHIP, CONTROL OR INFLUENCE RISKS ASSOCIATED WITH TECHNOLOGY VENDORS?

Novera contends that foreign ownership, control, or influence of technology vendors presents a present and material risk to Australia's cyber resilience and sovereignty.

Novera further calls the Government's attention to the influence of these foreign multinationals on public policy discourse. Many foreign operators employ registered lobbyists or internal advocacy teams to advance their commercial interests within the Australian policy environment. Beyond these unilateral activities, the same technology firms frequently provide financial support to so-called "peak bodies" which serve as additional vehicles for policy influence.

One such body, the Technology Council of Australia, whose membership includes a large number of foreign-owned multinationals, openly markets its association with past and present members of Federal and State parliaments in its collateral. Novera contends that such activity further underscores the risks of disproportionate influence on public policy by foreign interests in the technology sector.

Novera recognises that Australia will inevitably need to rely on foreign-owned technologies and service providers, given the nature of the technology sector and Australia's relatively minor role in the global technology industry. In many respects, Australia operates at the mercy of technology developments overseas. However, our position is that any risks associated with implementing and using foreign-owned technologies and service providers must be assessed, managed, and treated accordingly. This can only happen through transparency, visibility and trust.

Notwithstanding the above, Novera remains significantly concerned that the level of direct and indirect influence exercised by foreign-owned, controlled or influenced entities, or even the appearance of such influence, risks undermining public confidence in the neutrality of policy-making and regulatory design, where the overriding goal should be to ensure a safe and resilient society and economy. Without transparency and clear government guidance, Australian organisations, particularly SMBs and NFPs, struggle to identify, assess, and mitigate these dependencies.

RECOMMENDATIONS

Novera recommends that the Government develop:

1. **A Public Register of Critical Technology Vendors**: A transparent register disclosing beneficial ownership structures, foreign parent entities, and any foreign ownership, control or influence risks for technology vendors critical to national infrastructure.
2. **Guidance Aligned to International Best Practice**: Publish guidance aligned with standards such as ISO/IEC 27036 (Information Security for Supplier Relationships) covering practical steps to assess and mitigate foreign ownership, control or influence risk as part of vendor due diligence.
3. **Mandatory foreign ownership, control or influence risk risk assessments for Critical Infrastructure Operators**: Require operators of critical infrastructure to explicitly assess and report on foreign vendor dependency and influence, ensuring visibility of systemic concentration risks at the national level.

QUESTION 33

HOW EFFECTIVE DO YOU CONSIDER THE SOCI ACT AT PROTECTING AUSTRALIA'S CRITICAL INFRASTRUCTURE? ARE THE CURRENT OBLIGATIONS PROPORTIONATE, WELL-UNDERSTOOD, AND ENFORCEABLE?

Novera acknowledges the strategic importance of the SOCI Act as the cornerstone of Australia's critical infrastructure protection regime. Novera contends that the SOCI Act contributed to successfully elevating board and executive attention on security, broadened coverage across key sectors, and provided a legal foundation for the Government to act decisively in the national interest.

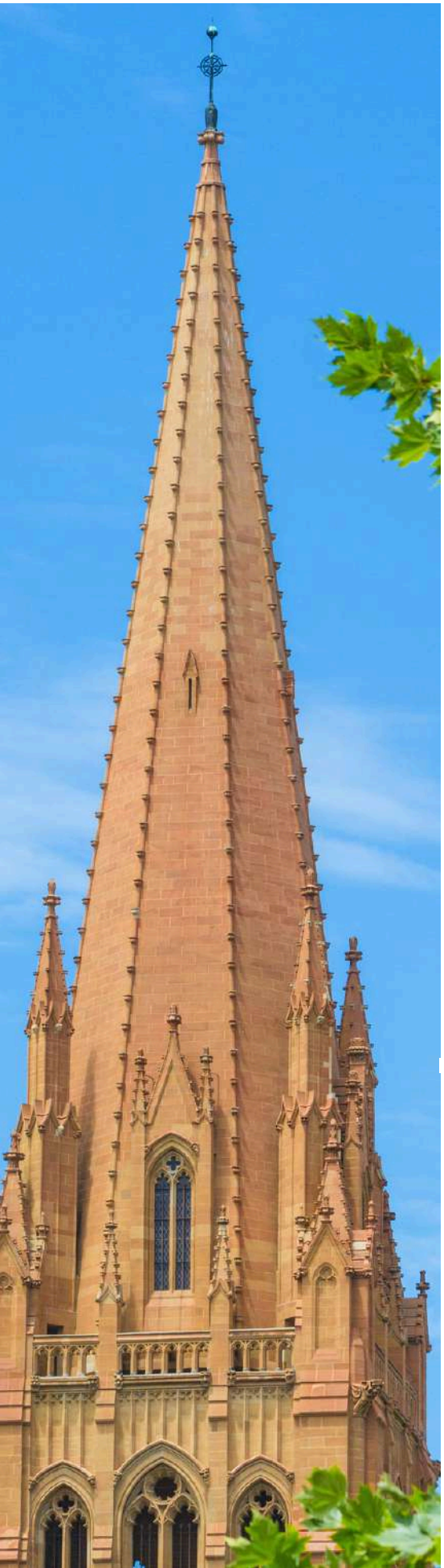
However, our experience indicates that execution challenges remain, which limit its overall effectiveness. These challenges include:

- **Alignment with International Standards**: Current SOCI Act guidance is not consistently aligned with international frameworks such as ISO/IEC 27001 or the NIST Cybersecurity Framework. This creates friction and duplication for entities already certified or operating under global standards, without necessarily delivering additional security outcomes.
- **Complexity for Smaller Entities**: Many smaller regulated operators and downstream service providers struggle to interpret and implement SOCI obligations without costly legal or technical support. This risks leaving parts of the supply chain under-prepared or exposed.
- **Balance of Enforcement and Support**: Enforcement capability is essential, but protection cannot be achieved through compliance activity alone. SOCI obligations need to be matched with education, maturity-appropriate guidance, and uplift funding to enable meaningful compliance.

RECOMMENDATIONS

To ensure the SOCI Act achieves its intent, Novera recommends the Government:

1. **Develop a Tiered, Standards-Aligned Implementation Framework**: Introduce a proportionate compliance model that reflects organisational size, sector, and maturity, with clear alignment to ISO/IEC 27001, the NIST CSF, and the ASD Essential Eight.
2. **Clarify Third-Party and Supply Chain Expectations**: Provide explicit guidance on how regulated entities should manage foreign ownership, control or influence (FOCI), subcontractors, and downstream dependencies. These expectations should be harmonised with other regulatory regimes such as APRA CPS 234 and any forthcoming Privacy Act reforms.
3. **Publish Tailored and Practical Guidance**: Issue guidance documents tailored to varying maturity levels and industry sectors. These should include plain-language resources, templates, and case studies to help entities translate obligations into practical steps.
4. **Balance Enforcement with Funded Uplift**: Create targeted uplift programs, grants, and subsidised cyber health checks for small and medium-sized operators in critical sectors, delivered by Australian-owned and operated service providers using AS/ISO 17024-accredited professionals who are certified against an Australian personnel accreditation scheme. This will ensure that obligations can be met in a competent and risk managed manner, without incurring disproportionate costs or administrative burdens.
5. **Pursue Harmonisation Across Regulatory Regimes**: Ensure alignment and consistency between SOCI, CPS 234, and Privacy Act reforms to minimise complexity and compliance fatigue, allowing entities to focus resources on genuine security outcomes.



QUESTION 39

WHAT ROLE SHOULD GOVERNMENT PLAY IN SUPPORTING THE DEVELOPMENT AND GROWTH OF AUSTRALIA'S CYBER WORKFORCE? WHAT INITIATIVES, PILOTS OR POLICY IDEAS DO YOU THINK WOULD BEST SUPPORT INDUSTRY TO GROW?

Australia's cybersecurity workforce is a cornerstone of national resilience. However, the sector remains fragmented and inconsistent, with a wide variation in qualifications, training pathways, and professional standards.

Unlike other critical professions such as law, medicine, and accounting, cybersecurity has yet to achieve formal recognition as a regulated profession with defined minimum standards.

As argued by Tony Vizza and Professor Jill Slay AM in the paper 'A Proposal for a Professional Recognition Scheme for the Australian Cyber Security Profession',[1] this lack of consistency leaves Australia exposed to widespread and systemic risks.

These risks include:

- Organisations cannot always distinguish between competent professionals and those without relevant qualifications or experience.
- Training and certification pathways are inconsistent, with a proliferation of low value, poor quality and non-accredited courses diluting the market.
- There is limited accountability for individuals operating in the sector who provide poor quality or misleading advice.
- Workforce mobility, both domestically and internationally, is constrained by the absence of universally recognised standards.

Novera contends that Government leadership is essential to address this gap. The most effective role for Government is to embed professionalisation of the cyber sector into policy and regulation, supported by pathways that enable sustainable workforce growth and diversity.

[1] Tony Vizza and Jill Slay, *A Proposal for a Professional Recognition Scheme for the Australian Cyber Security Profession,* January 2025 <https://novera.com.au/wp-content/uploads/2025/01/A-Proposal-for-a-Professional-Recognition-Scheme-for-the-Australian-Cyber-Security-Profession-Tony-Vizza-and-Jill-Slay-AM-January-2025_C-1.pdf>.

RECOMMENDATIONS

Novera recommends that the Government undertake the following:

1. **Legislate a Cybersecurity Professionalisation Framework**: Create a statutory framework, comparable to accounting or engineering, with protected professional titles, minimum competency standards, and oversight via a recognised guidance body. Adopt a staged approach which includes:
    - Stage 1 (Voluntary): Government endorsement; procurement preferences for certified practitioners.
    - Stage 2 (Targeted Mandate): Minimum standards required for defined advisory/assurance roles in government and critical sectors.
    - Stage 3 (Protected Titles): Legal protection of titles such as "Chartered Cybersecurity Professional" tied to ethics and continuing professional development (CPD) obligations.

This trajectory mirrors the governance model proposed by Vizza and Slay.[2]

2. **Endorse AS/ISO/IEC 17024-Accredited Certifications as the Baseline**: Formally recognise appropriate AS/ISO/IEC 17024 personnel certifications as the minimum benchmark for advisory, audit, and risk roles. Codify this in policy and procurement to curb the proliferation of non-accredited training and align with the Vizza and Slay Scheme's Pathway One (fast-track via AS/ISO/IEC 17024).[2]

3. **Stand Up a National Body and Register**: Establish (or appoint) a not-for-profit body to administer criteria, recognition, complaints, and ethics; and to run a public register of certified professionals that gives employers/regulators confidence in verified competence and good standing. The composition and remit should reflect the paper's industry–government–academia working group design, with clear interfaces to ASD/ACSC, DISR, DHA and state governments.

4. **Dual Pathways to Professional Recognition (Inclusive On-Ramps)**: Implement two inclusive pathways, as proposed by Vizza and Slay:[2]
    - Pathway One: AS/ISO/IEC 17024-accredited certifications which included verified paid and hands on work experience (fast-track).
    - Pathway Two: Competency-points route that recognises tertiary study, vendor-neutral training, verifiable work experience, and background/character checks, mapped to practice levels (Associate, Principal, Chartered) and to frameworks like ASD Cyber Skills Framework and SFIA.

[2] Tony Vizza and Jill Slay, *A Proposal for a Professional Recognition Scheme for the Australian Cyber Security Profession,* January 2025 <https://novera.com.au/wp-content/uploads/2025/01/A-Proposal-for-a-Professional-Recognition-Scheme-for-the-Australian-Cyber-Security-Profession-Tony-Vizza-and-Jill-Slay-AM-January-2025_C-1.pdf>.

RECOMMENDATIONS

5. **Fund Bridging and Micro-Credential Pathways** (Stackable, Standards-Mapped): Co-fund short, stackable micro-credentials, mapped to practice areas (Incident Response (IR); Governance, Risk and Compliance (GRC); privacy; AI risk; digital forensics, etc) to help IT, risk, engineering and legal professionals transition into cyber. Tie micro-credentials to the national body's competency map and to AS/ISO/IEC 17024 certification tracks to ensure portability.

6. **Support SMB-Focused Cyber Capability Hubs**: Create regional/sectoral hubs that offer subsidised secondments, shared services (IR, testing, assessments), and mentoring by registered professionals—so SMBs and NFPs can access trustworthy expertise and so early-career professionals can accrue supervised, verifiable experience.

7. **Keep Costs Low and Leverage What Works**: Adopt the principles incorporated in Vizza and Slay professionalisation proposal paper, which include minimal cost to individuals, no new duplicative certifications, recognition of hands-on experience, a code of ethics, and continuing education to maintain currency.[3] This ensures the scheme scales, remains vendor-agnostic, and delivers measurable uplift.

LINK TO HORIZON 2 GOALS

This program advances Horizon 2 by scaling cyber maturity, strengthening sovereign capability, and growing a diverse, professional workforce. Professionalisation, implemented through AS/ISO/IEC 17024 standards, a national register, and inclusive pathways, turns fragmented training markets into a trusted profession with clear entry, mobility, and accountability.

[3] Tony Vizza and Jill Slay, *A Proposal for a Professional Recognition Scheme for the Australian Cyber Security Profession,* January 2025 <https://novera.com.au/wp-content/uploads/2025/01/A-Proposal-for-a-Professional-Recognition-Scheme-for-the-Australian-Cyber-Security-Profession-Tony-Vizza-and-Jill-Slay-AM-January-2025_C-1.pdf>.

QUESTION 49

IN WHICH FORUMS AND ON WHICH ISSUES WOULD YOU LIKE AUSTRALIA TO FOCUS EFFORTS TO SHAPE RULES, NORMS AND STANDARDS IN LINE WITH ITS INTERESTS MOST EFFECTIVELY IN HORIZON 2?

Novera contends that Australia's ability to shape the global rules-based order in cyberspace depends on active participation in multilateral forums, regional groupings, and standards-setting bodies. Horizon 2 presents an opportunity for Australia to leverage its reputation as a trusted middle power, its strong alliances, and its growing cyber capability to influence the design of rules, norms, and standards in ways that protect national sovereignty, support democratic values, and reduce systemic risks.

Novera contends that Australia should focus its diplomatic and policy energy on the following priorities:

1. UN Convention on Cybercrime

Australia should continue to play a leadership role in supporting the adoption and effective implementation of the UN Convention on Cybercrime. Our priorities should include:

- Ensuring strong enforcement mechanisms to prevent safe havens for cybercriminals.
- Embedding procedural safeguards to balance law enforcement needs with privacy, due process, and human rights.
- Safeguarding digital sovereignty by ensuring that evidence-sharing and jurisdictional provisions respect national legal frameworks.

2. AI Governance Standards

Australia should engage actively in ISO, OECD, and UN-led AI governance initiatives to shape standards around:

- Secure and ethical development of AI systems.
- Transparency, explainability, and auditability in AI decision-making.
- Embedding safety-by-design and accountability principles into global frameworks.
- This would ensure Australia is not simply a passive taker of foreign standards but an active contributor to rules that reflect democratic values and risk management priorities.

3. Foreign Control of Digital Infrastructure and Services

Australia should lead international efforts to address foreign ownership, control, or influence of critical digital infrastructure and services, including hyper-scale cloud, cybersecurity platforms, software supply chains and critical service providers. Diplomatic initiatives should promote:

- Joint transparency standards for vendor ownership and control.
- Risk assessment protocols for governments and critical operators.
- Collaborative approaches to managing systemic dependency on a small number of foreign technology multinationals.
- Harmonisation of taxation regimes to ensure that Australian-based digital infrastructure commercial entities and services are not at a commercial disadvantage compared to foreign-owned multinationals that leverage tax minimisation and profit offshoring schemes to reduce their tax liabilities while having the ability to undercut Australian entities for deals.

4. Interoperable Cybersecurity Standards

Australia should advocate for alignment between national and international standards and frameworks to:

- Reduce regulatory friction for globally integrated businesses.
- Lower compliance costs for SMEs seeking to export.
- Promote trust in Australian goods and services in the international market by demonstrating adherence to internationally harmonised standards.

5. Digital Services Tax and Technology Fair Contribution

Australia should advance proposals for a digital services tax levied at the point of transaction at the OECD and G20 levels, ensuring that global technology multinationals contribute fairly to the Australian digital economy.

Novera argues that tax revenues generated from any digital services taxes should be ring-fenced and used to support local capability, innovation, and workforce development, enhancing sovereign resilience while levelling the playing field for Australian companies.

6. ASEAN, Quad, APEC and Pacific Cooperation and Capacity Building

Work with ASEAN, Quad, APEC and Pacific partners and regional cyber centres to:

- Stand up or strengthen national CSIRTs, run joint exercises, and publish shared incident playbooks (ransomware, BEC, supply-chain).
- Develop and issue sector toolkits (OT/ICS security for water, energy and health sectors) mapped to ISO/NIST/E8.
- Coordinate crypto-tracing and asset recovery, sanctions on enablers, and a joint extortion-reporting baseline to accelerate disruption operations across jurisdictions.
- Support harmonised cybercrime legislation and rapid evidence-sharing practices to shorten response times.
- Enhance subsea cable security and contingency communications for resilience.

RECOMMENDATIONS

Novera recommends that the Federal Government:

1. Champion the UN Convention on Cybercrime with a focus on enforcement, safeguards, and sovereignty.
2. Shape AI governance standards at ISO, OECD, and UN forums to reflect secure, transparent, and ethical development.
3. Lead international efforts on foreign ownership transparency for critical digital infrastructure and seek to harmonise corporate taxation regimes to ensure Australian born and based entities are not at a commercial disadvantage.
4. Advocate for interoperable cybersecurity standards (ISO/NIST) to reduce friction and strengthen trust in Australian exports.
5. Advance a digital services tax at OECD/G20 levels to ensure global technology firms contribute proportionately to Australia's digital ecosystem.
6. Constructively work with and cooperate with our regional partners in ASEAN, the Quad, APEC and the Pacific.

LINK TO HORIZON 2 GOALS

Enhancing the SOCI Act through harmonisation, proportionate compliance models, and practical support will directly advance the Horizon 2 objectives of scaling cyber maturity across the economy, strengthening sovereign capability, and investing in the broader cyber ecosystem. By streamlining obligations and embedding international standards, the Act can deliver more effective protection of critical infrastructure while reducing unnecessary compliance burden.

ABOUT NOVERA

WHO WE ARE

Novera is a specialist Australian-owned and operated advisory firm that helps organisations protect, optimise, and govern their digital assets. We empower clients to manage risk, achieve compliance, and operate securely in an increasingly complex regulatory and threat environment. With over 20 years of hands-on experience, our team brings unrivalled expertise in cybersecurity, artificial intelligence (AI), and information technology (IT).

WHAT WE DO

We provide pragmatic, actionable and independent advice tailored to each client's operational needs. Our services include:

- **Cybersecurity**: Strategy and roadmap development; risk and maturity assessments aligned to industry frameworks and standards, ISO/IEC 27001 readiness; third-party and M&A due diligence; Fractional CISO services; Board and C-Suite governance support.
- **Artificial Intelligence**: AI risk management; ISO/IEC 42001 compliance; regulatory advisory; AI cybersecurity and privacy assurance; Board and C-suite consulting.
- **Information Technology**: IT strategy and transformation; governance and compliance support; IT audit and assurance; Fractional CIO services.
- **Expert Evidence**: Independent expert reports, testimony, and consulting support for litigation, regulators, and government.

OUR EXPERIENCE

Novera has successfully advised and assisted ASX-listed entities and multinational organisations; Regulators, law firms, and governments (federal and state); APRA- and SOCI-regulated firms; Financial services, superannuation, and insurance providers; High-risk small and mid-market businesses; and large national and international not-for-profits

WHAT MAKES US DIFFERENT

- Impactful and pragmatic: we provide advice that is immediately actionable.
- Client-focused: our success depends on delivering the right outcomes and results that our clients need.
- Trusted expertise: we are recognised leaders in AI, cybersecurity, and IT risk management, with globally respected and coveted certifications, qualifications and experience at the most senior levels.

OUR PEOPLE

Our team hold degree qualifications in IT, computer science, business administration, and law from leading institutions in Australia and across the world. Our team of accomplished and trusted experts hold some of the highest levels of IT, cybersecurity, risk management and legal qualifications, honours and experience available today.

LEGAL INFORMATION

1. The views and opinions expressed in this document are those of Novera and do not necessarily reflect the official policy or position of any entity referred to within this document. Examples of analysis performed within this document are only examples.
2. While care and consideration has been taken in the creation of the material in this document, Novera does not warrant, represent, or guarantee that the material published in this document is in all respects accurate, complete, and current. To the fullest extent permitted by law, any liability, including any liability for negligence, for any loss or damage arising from reliance on material in this document, is excluded.
3. Except as permitted by copyright law, you may not reproduce, distribute or communicate any of the content in this document, without the express written permission of the copyright owner.
4. The Australian Copyright Act allows certain uses of content without the copyright owner's permission. This includes uses by educational institutions for educational purposes and by Commonwealth and State government departments for government purposes, provided fair payment is made.
5. This document is copyrighted material owned by Novera. This document or its contents may not be reproduced, distributed, or displayed in any form, without proper attribution.

ABOUT THIS DOCUMENT

Novera's submission to the Horizon 2 consultation of the 2023–2030 Cyber Security Strategy calls for decisive action to address systemic risks in Australia's digital ecosystem. It emphasises five priorities: embedding AI governance to counter malicious use, reducing foreign dependency and enhancing digital sovereignty, making cyber resources usable for SMBs and NFPs, harmonising regulatory regimes while enacting Privacy Act reforms in full, and legislating the professionalisation of the cyber workforce through AS/ISO/IEC 17024-aligned standards.

Novera also urges Australia to lead globally by championing the UN Convention on Cybercrime, shaping AI and cybersecurity standards in ISO, OECD, and UN forums, advancing a digital services tax at the OECD and G20, and deepening Indo-Pacific cooperation through ASEAN, Quad, APEC, and Pacific partnerships. Together, these measures will scale national cyber maturity, strengthen sovereign capability, and position Australia as a credible global leader in Horizon 2.

novera

[redacted]

Web: www.novera.com.au