Response to 2023-2030 Australian Cyber Security Strategy Discussion Paper

April 2023

tesserent

tesserent

Mr Andrew Penn, Mr Mel Hupfeld and Ms Rachael Falk
Expert Advisory Board
2023-2030 Australian Cyber Security Strategy
Australian Government

14 April 2023

Re: Response to 2023-2030 Australian Cyber Security Strategy Discussion Paper

Dear Expert Advisory Board

Tesserent welcomes the Australian Government initiative to develop a 2023-2030 Australian Cyber Security Strategy. With an ever-evolving digital landscape and our increasing dependence on digitally-complex environments, we believe this is a crucial time to focus on domestic and international cyber security.

Tesserent Limited is an ASX listed company. From 2019 to 2023 we acquired thirteen (13) cyber security companies to create a comprehensive range of cyber security services. Our foremost priority is to monitor, safeguard and defend digital assets.

Our clients are based primarily in Australia and New Zealand, serviced by a growing team of approximately 500 cyber security professionals, technicians and staff across both countries. As a direct result of this expansion we are a leading supplier of cyber security services to over 1300 government, commercial and critical Infrastructure clients. We support our client base with strategic advice, testing, monitoring security services and product controls.

For the last 20 years, Australia's approach to cyber security has been responsive, based on emerging threats and risks. Unlike our military and civil defence, which has an overarching set of goals and strategies, cyber security has complex legislation and a diverse range of recommendations and standards. For example, while the SOCI Act and Essential Eight are both excellent, there is a lack of coherence that makes the cyber security regulatory environment extremely complex.

Skills development is a major area of concern. Even with a world-leading strategy, our capacity to execute will be limited unless we make significant investments and change our national approach to how we encourage people to take up a career in cyber security, train them and support their ongoing education.

The opportunity to provide feedback to the recently released 2023-2030 Australian Cyber Security Strategy Discussion Paper is exciting. We believe that Tesserent can add significant value in three key focus areas. These include:

- Building a national resourcing strategy
- Supporting whole-of-government investment
- Elevating sovereign Australian capability

This submission responds to these focus areas and lists our recommended priorities for action.

We are grateful for the opportunity to express our expertise and offer perspectives on the necessary measures to position Australia at the forefront of cyber security by 2030.

Our board of directors and leadership teams look forward to working in partnership towards this shared vision and securing our digital future, together.

If you would like to discuss any aspects of our response, please don't hesitate to contact me directly at [redacted]

Yours sincerely

[redacted]

Kurt Hansen
Chief Executive Officer
Tesserent Limited

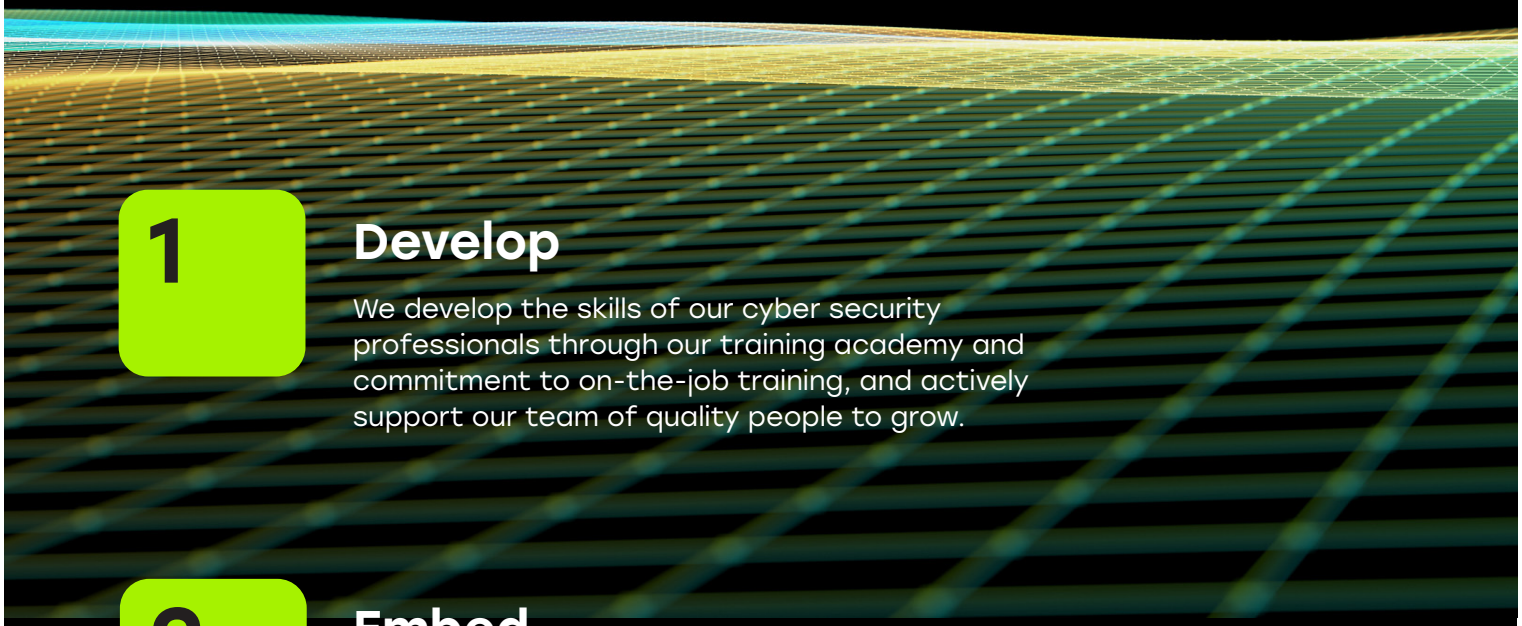
A shared vision

To be the world's most cyber secure country by 2030, we need the unified effort of government, industry and the community.

Tesserent

We appreciate the opportunity to share our industry perspectives and priorities for action. Tesserent has a track record of supporting cyber security challenges in Australia with a strong commitment to:

1. **Develop**
2. **Embed**
3. **Innovate**



1 Develop

We develop the skills of our cyber security professionals through our training academy and commitment to on-the-job training, and actively support our team of quality people to grow.

2 Embed

We integrate our cyber security capabilities and protections into the functional areas of organisations every day. From software and product development, to finance, business analysis, marketing, investor relations and reputation management.

3 Innovate

We invest in local talent to uphold cyber security skills, promote scalability and sustainability. We bolster local capabilities in sovereign-based intellectual property through innovation and funding.

A unified effort … securing our digital future, together

National resourcing strategy

Grow Australia's cyber security workforce

Supporting the growth of our future cyber security workforce through education, encouraging skilled immigration and accreditation is a key imperative for government and industry.

Whole-of-government investment

Support coordinated investment outcomes

Proactive support and investment across all tiers of government is critical to achieve broader and consistent outcomes that minimise risk.

Sovereign Australian capability

Elevate local infrastructure and IP capability

Supporting collaboration with allies and investment in home-grown capabilities and intellectual property is key to maintaining control over our own data to counter interference.

National resourcing strategy

Grow Australia's cyber security workforce

Supporting the growth of our future cyber security workforce through education, encouraging skilled immigration and accreditation is a key imperative for government and industry.

PRIORITIES FOR ACTION

EDUCATION

- Jump start Australia's talent pool by working in partnership with Year 11 and 12 subject educators to embed cyber security fundamentals in the curriculum.
- Create industry pathways through apprenticeship programs and supported industry placements.
- Uplift cyber skills and support more specialised career pathways through nuanced skills development.
- Expand from tertiary degrees to micro certifications and recognition of prior learning, work and life experience.

INCENTIVES

- Inject more skilled resources to the cyber security ecosystem.
- Offer tax and/or grant incentives for sovereign providers to support new hires and upskilling programs.
- Encourage career moves through a combination of subsidies, training and mentoring programs, as well as streamlined immigration policies.

DIVERSITY

- Accelerate the support, enablement and training of a more inclusive and diverse workforce in cyber security.

POLICY IN ACTION

Supporting women in cyber security

Women currently represent only 16 per cent of the Australian cyber security industry workforce*. Through our partnerships with the Australian Women in Security Network and OxCC (a cyber security training conference for women, by women), and engagement with industry and technical partners, Tesserent is accelerating the support, enablement and training of women in cyber security.

We take great pride in our commitment to inclusivity and diversity, as demonstrated by our business having over 25 per cent more women than the national average of 16 per cent*.

*Source: Australian Cyber Security Magazine: Women in Australia's Cyber Security Industry Growing here, October 2022.

Discussion Paper questions 1, 6 and 12 addressed.

Whole-of-government investment

Support coordinated investment outcomes

Proactive support and investment across all tiers of government is critical to achieve broader and consistent outcomes that minimise risk.

PRIORITIES FOR ACTION

CONTRACTING

- Mobilise public-private partnerships to leverage staff expertise, accelerate and streamline cross-agency security clearance and portability to improve onboarding times.
- Shift towards outcome-focused contracting to prioritise objectives over time-based methods.
- Leverage federal purchasing power by sourcing tools and automation for best practice outcomes.

RISK

- Regain senior leadership attention with a focus on consequence of risk and to better understand mitigation approaches.
- Identify common services to be secured across all tiers of government.
- Apply consistent controls across agencies.

INCIDENT RESPONSE

- Implement an accreditation scheme for organisations delivering threat response capabilities in the Australian market to ensure adherence to best practice standards during and after incidents, modelled on the current Infosec Registered Assessor Program (IRAP) assessments and evaluate its effectiveness.
- Enhance the Critical Infrastructure Act, with the Australian Government taking the lead on this scheme (similar to IRAP).

INDUSTRY INSIGHT

Investment for better coordination across government tiers

Legislation and government advice is fractured. While the quality of information is high, there is a lack of integration and coherence with different compliance and regulatory regimes. Greater coordination, unified under a strong strategic intent, like that of the civil and military defence force, is imperative.

Cyber is approached as a business-as-usual activity, subject to efficiency dividends and funding issues. Home Affairs recently received no new funding to set up a national office for cyber security. In contrast, government invested heavily in centralised capability in the REDSPICE Program.

A broader cyber uplift program should include coordination and investment across federal, state and local government and match the REDSPICE investment.

Discussion Paper questions 1, 2b, 2d, 3, 6, 12 and 18 addressed.

Sovereign Australian cyber capability

Elevate local infrastructure and IP capability

Supporting collaboration with allies and investment in home-grown capabilities is key to maintaining control over our own data to counter interference.

PRIORITIES FOR ACTION

COLLABORATE

- Commence risk assessment of foreign partners and suppliers to ensure long term support and relationships established with partner countries such as AUKUS and Five Eyes alliance.

DESIGN

- Leverage existing research across the Five Eyes alliance to design new technologies.
- Invest in Australian intellectual property to support national intelligence and defence community to counter rising threats from overseas and criminal actors.
- Enhance security in new technologies to maintain strategic flexibility in their use.

REGULATION

- Streamline regulatory frameworks to ensure the safety of technology use by holding stakeholders accountable and promoting transparency in the technology creation process.

GLOBAL TREND

A panel of global technology experts including leading tech entrepreneurs Elon Musk and Steve Wozniak, raised concerns about the rapid pace of development and access to artificial intelligence (AI). They called for a pause in its availability until shared safety protocols are implemented and robust AI governance frameworks and systems are developed collaboratively between developers and policymakers. Additionally, AI ethicists are raising concerns about exploitative practices in developed technology.

An Australian Government funded initiative in partnership with industry is needed to develop and test algorithms that protect applied AI models from existing vulnerabilities. The initiative should focus on researching how AI algorithms can be protected from cyber attacks. Governance frameworks and enhanced regulations are essential to ensure this emerging technology is used appropriately, to benefit society and human rights.

Discussion Paper questions 1, 2a, 3, 4, 5, 6, 15, 16 and 19 addressed.

Securing our digital future, together

National resourcing strategy

Grow Australia's cyber security workforce

Areas for action:

- Education
- Incentives
- Diversity

Whole-of-government investment

Support coordinated investment outcomes

Areas for action:

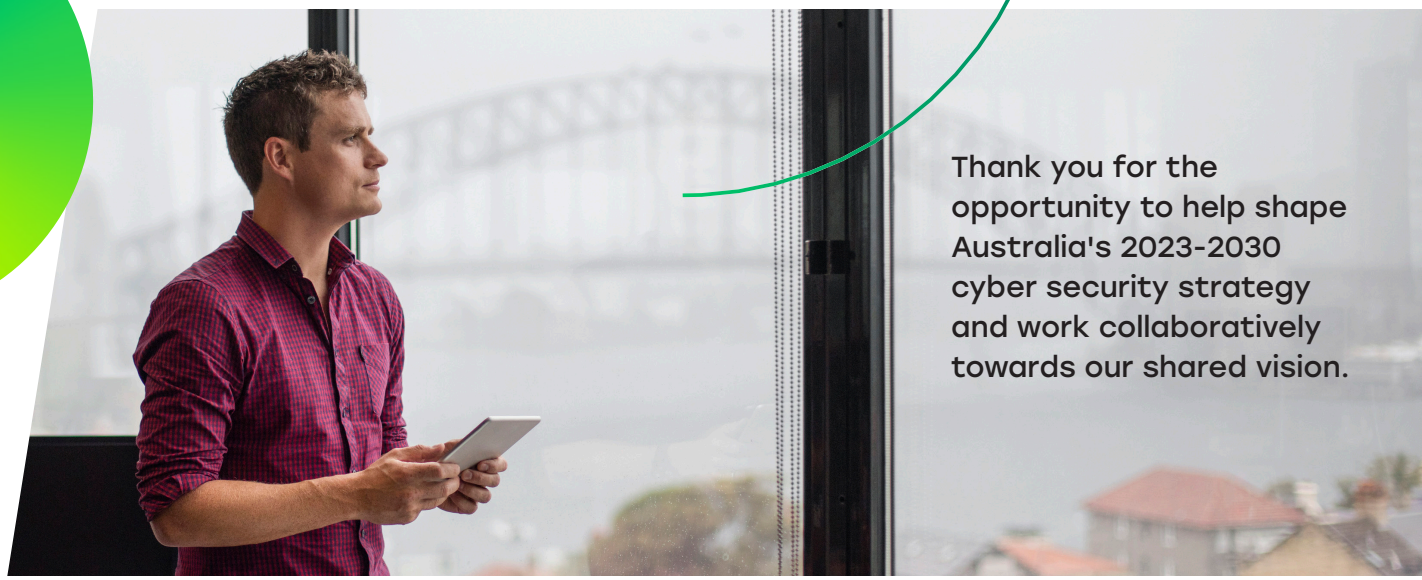
- Contracting
- Risk
- Incident Response

Sovereign Australian capability

Elevate local infrastructure and IP capability

Areas for action:

- Collaborate
- Design
- Regulation



Thank you for the opportunity to help shape Australia's 2023-2030 cyber security strategy and work collaboratively towards our shared vision.

Tesserent Limited

Level 5, 990 Whitehorse Road
Box Hill, VIC 3128, Australia

Phone: +61 3 9880 5555
Email: info@tesserent.com

tesserent