ACT Government

[redacted]

The Hon Tony Burke MP
Minister for Home Affairs and Cyber Security
Parliament House
CANBERRA ACT 2600

Our ref: PRO25/3655

Via email: Tony.Burke.MP@aph.gov.au; DLO.Burke@homeaffairs.gov.au

Dear Minister Tony

I write in relation to the Department of Home Affairs Consultation Paper on *Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy* (the Consultation Paper). Thank you for the opportunity to input on the development of this second stage of implementation of Australia's Cyber Security Strategy.

The ACT Government is in-principle supportive of the Australian Government's ambition to make Australia the world's most cyber secure nation by 2030. We recognise the important work in Horizon 1 of the Strategy which aimed to strengthen foundations and address critical gaps in our cyber posture.

We support the goals of Horizon 2 to expand the reach to small and medium businesses, non-for-profit organisations, education and other sectors to uplift cyber security capability and resilience across the economy. To achieve the success will require an ongoing engagement with all sectors and a truly national approach to working together with state/territory governments on improving cyber security across society.

The ACT Government Submission provides a range of feedback and recommendations on the Consultation Paper at Attachment A.

I look forward to continuing to work together on making Australia a world leader in cyber security.

Yours sincerely

[redacted]

29 August 2025

ACT Legislative Assembly
[redacted]

Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy – Policy Discussion Paper

ACT Government Submission

ACT Government

Acknowledgement of Country

The ACT Government acknowledges the Ngunnawal people as traditional custodians of the ACT and recognise any other people or families with connection to the lands of the ACT and region.

We respect the Aboriginal and Torres Strait Islander people, particularly our Aboriginal and Torres Strait Islander staff, and their continuing culture and contribution they make to the Canberra region and the life of our city.

Produced by the ACT Government. Enquiries about this publication should be directed to the ACT Government.

GPO Box 158, Canberra City 2601
act.gov.au
Telephone: Access Canberra – 13 22 81

If you are deaf, or have a hearing or speech impairment, and need the telephone typewriter (TTY) service, please phone 13 36 77 and ask for 13 22 81.

For speak and listen users, please phone 1300 555 727.

For more information on these services, contact us through the National Relay Service: www.accesshub.gov.au.

If English is not your first language and you require a translating and interpreting service, please telephone Access Canberra on 13 22 81.

Contents

Introduction

The ACT Government welcomes the opportunity to respond to the Policy Discussion Paper - Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy.

This ACT Government (the ACT) is in-principle supportive of the Australian Government's ambition to make Australia the world's most cyber secure nation by 2030. This submission sets out our perspective to inform development of *Horizon 2 of the 2024-2030 Australian Cyber Security Strategy* (the Discussion Paper) to scale cyber maturity across the whole economy.

We recognise the important work in Horizon 1 of the Strategy which aims to strengthen foundations and address critical gaps in our cyber shields, build better protections for our most vulnerable citizens and businesses, and support the cyber maturity uplift across the region.

Of the well-known challenges in cyber security, one is paramount: many organisations and individuals do not have the skills, technology, and resources (financial or otherwise) to adequately protect themselves and their stakeholders or customers.

To achieve this whole-of-nation, whole-of-economy vision, the development of initiatives under *Horizon 2* should focus on:

- undertaking a holistic approach to review the current scope of regulatory reforms across cyber, privacy, data and identity; and assess the cumulative impacts and costs to business and industry sectors
- providing leadership and guidance in the uptake of emerging technology, such as Artificial Intelligence (AI)
- prioritising support to businesses and sectors which have limited cyber literacy and resources
- prioritising addressing vulnerabilities that have the greatest potential for harm to the community.

Highlights of the ACT submission and recommendations are:

- **Shield 1:** Providing resources and support to uplift cyber security and resilience among small and medium-sized businesses and NFP organisations; partnering with sub-national governments to support a sustainable and diverse cyber workforce and local cyber business ecosystem; and developing a national approach on cyber messaging and cyber literacy curriculum to help long term cyber security awareness and preparing future cyber workforces.
- **Shield 2:** Providing leadership and guidance in the responsible and safe uptake of emerging technology, such as AI; and prioritising to address vulnerabilities of high risk technologies and data collection practices that have the greatest potential for harm to the community, especially digital identity and sensitive personal information of our citizens.
- **Shield 3:** Increasing data sharing of assessments under the Technology Vendor Review Framework (TVRF).

- **Shield 4:** Ongoing development with sub-national governments to take a truly national approach to protecting what is critical.
- **Shield 5:** Providing funding support that strengthen the workforce in critical and emerging industries; and developing sovereign capabilities through procurement opportunities to local SMEs, particularly defence-related industry.
- **Shield 6:** Nil response.

State/Territory governments have a critical role in protecting critical government services; protecting the community from the harm caused by cyber incidents, supporting local industry and business sectors; and enabling the next generation of cyber competency and literacy.

Making Australia the most cyber safe nation requires a collaborative approach. The Commonwealth should continue to engage and partner with sub-national governments to develop practical strategies and initiatives. Furthering consultation to key sectors to ensure that new regulations are sustainable and capable of achieving stated objectives across government, industry, business and the NFP sector. This will empower governments in all levels, and sectors across the economy to build a strong cyber security culture and resilience.

ACT Government Response to the Discussion Paper

2. Developing our vision for Horizon 2

2.1 Outlook for Horizon 2

Cyber threats continue to evolve, driven by a rapid advancement in cyber space, increasingly accessible emerging technologies, and ever more interconnected digital systems and infrastructure. In alignment with Australia's ambition to be a world leader in cyber security by 2030, the Commonwealth should continue to take a lead role in ensuring safe and secure adoption of emerging technologies such as AI, to safeguard our digital infrastructure, systems, and applications, and protect the digital identity and sensitive information of our citizens.

In considering the current global threat environment, attention should be given to reports of growing public distrust in institutions, which was highlighted by the *2025 Edelman Trust Barometer Global Report*. Efforts to uplift security culture and awareness are increasingly challenged by a complex threat landscape and shifting public perceptions of institutional ethics and effectiveness, shaped by media narratives and personal experiences. Strengthening cyber security and resilience presents an opportunity to strengthen public trust, especially given the risks associated with compromised sensitive information.

Recommendation:

- That the Commonwealth continue to lead on national approaches to the safe adoption of emerging technologies to maintain public trust, safeguard digital infrastructure, and protect sensitive personal information of citizens.

2.2 Collaborating across all levels of Australian Government

To create the broader whole-of-economy changes sought by the Cyber Security Strategy requires strong partnership with sub-national governments on a national approach to solving challenges and safeguarding future innovation and adoption of new technologies.

The ACT benefits from initiatives like the Trusted Information Sharing Network (TISN) to bring together peers across government and industry to connect and learn together. These forums offer space and opportunity for information sharing, particularly to encourage sub-national governments to share and learn from others the best-practice cyber security governance and practice.

To enhance cyber resilience, it is important to recognise the continuous support and influence of sub-national governments who have a critical role in protecting critical government services; protecting the community from the harm caused by cyber incidents, supporting local industry and business sectors; and enabling the next generation of cyber competency and literacy.

There is an ongoing challenge especially the lack of resourcing for many public sector organisations, particularly non-Commonwealth entities. The lack of financial resources does not just impact staffing, it also impacts what uplift is possible and in what timeframes. The ACT is adopting a risk-based approach to cyber security that requires constant consideration of value proposition.

Addressing cyber security resilience through increased legislative requirements will greatly exacerbate this issue for most public sector entities and businesses and must be approached with exceptional caution. Further consultation and development efforts would ensure that initiatives are sustainable and capable of achieving their stated objectives within jurisdictions.

Recommendation:

- That the Commonwealth continue the engagement with State/Territory governments as key partners, especially when developing policies and legislative reforms to achieve the outcomes in the *Cyber Security Strategy*.

2.3 Monitoring progress in a changing world – a conceptual framework for evaluating cyber security outcomes.

The ACT supports the *Cyber Security Policy Evaluation Model* to provide timely, responsive, and agile approaches to learning lessons and responding to the evolving cyber security landscape.

Cyber threats continue to evolve, driven by a rapid advancement in cyber space, increasingly accessible suite of emerging technologies, interconnected digital systems and infrastructure, at both a local and regional scale. This proliferation presents both challenges and opportunities in an evolving cyber threat environment, highlight the importance of a concerted, holistic and collaborative effort from governments, industry, and community alike.

To build national cyber resilience and boost cyber security across the economy, other non-cyber security contributing factors and lessons learnt from other policy areas, such as supply chain risks, should be considered in the policy evaluation model.

Recommendations:

- That the Commonwealth consider other non-cyber factors and lessons-learned from other policy areas to inform the *Cyber Security Policy Evaluation Model.*
- That the readability of the model is improved to support a clearer understanding of how evaluation (and its related scale) is determined.

3. Shield-level focus for Horizon 2

3.1 Shield 1: Strong businesses and citizens

Consolidating cyber awareness messaging across the economy

To build consistent and targeted cyber awareness campaigns, the Commonwealth should adopt a single national cyber brand and expanding multilingual and minority-community tailored outreach programs. The Commonwealth should produce white-labelled, open-source content where possible so that it can be easily adapted by government, industry, and community organisations; for example, standardised SCORM e-learning software products, creating modules suitable to different learning

management systems. This approach supports tailored outreach, especially for culturally and linguistically diverse (CALD), remote, and minority communities.

Cyber literacy will be a fundamental skill for the younger generations. To build cyber literacy and awareness across society, cyber safety and digital resilience should be embedded into the national curriculum at all education levels, from early childhood to tertiary education. This requires the development of age-appropriate resources in collaboration with educators, national-level curriculum support that integrates cyber literacy, and ongoing professional development for teachers to deliver this content effectively. Considering gamification in the design of these educational materials may support the engagement and uptake of these programs. Together, these efforts will help to equip students and educators with the skills and knowledge needed to navigate the digital world safely and confidently.

Supporting small and medium-sized businesses

The Commonwealth should prioritise resilience uplift for small to medium-sized enterprises (SMEs) that lack the capacity to adequately protect themselves, including through the provision of low or no-cost baseline cyber security standards that are practical and accessible.

Supporting small and medium-sized businesses to strengthen their cyber security continues to be crucial to supporting business resilience and capability uplift. We have heard from ACT business stakeholders that they recognise the importance of raising business awareness and developing capability for local businesses to understand risks associated with cyber security. Key risks they have identified include:

- Open ecosystems which facilitate entrepreneurial activity may be susceptible to foreign interference
- Outsourcing work overseas, such as information technology (IT) or accounting services, where businesses may not be aware of the risks associated with these practices
- The challenges for small businesses to invest in data protection, and
- Information not being accessible or concise for the business community.

In line with national conversations about productivity, it must be recognised that three out of five small businesses do not employ staff and are time poor. It is recommended that any measures that are proposed are delivered in a way that acknowledges and allows for these pressures on small businesses.

With the increasing regularity and breadth of cyber security breaches, business and governments face a constantly growing threat to digital security. Everyday businesses are faced with a previously unrecognised need to adopt data and cyber security protection into their business models.

AI has already shown its ability to drastically alter how business is carried out in areas, such as improving customer-facing applications to optimizing back-office efficiency, and incorporating data-driven insights throughout the entire business ecosystem. Noting this, there are concerns that AI will increase the risk around sensitive information being leaked or stolen and that AI use may be found to violate laws or regulations in various jurisdictions. Given AI is a tool that enhances productivity and provides streamlined ways of delivering skills and knowledge, the Commonwealth should assist in guiding uptake and knowledge of cyber security awareness, and the responsible and safe use of emerging AI technology.

The ACT regularly promotes Commonwealth programs and services for small businesses to help improve their digital skills and cyber security knowledge and resilience. For example, the ACT facilitated introductions to key local business organisations for the Digital Solutions program. Digital Solutions now runs regular workshops for businesses in collaboration with these organisations. A local Cyber Wardens case study featured in the ACT's Business e-newsletter.

Further localised case-studies and other dedicated promotional material from the Commonwealth services, particularly where businesses are supported to successfully improve their cyber security can be shared by the ACT through direct and stakeholder channels.

The ACT's approach to promotion and training recognises the time poor nature of small business owners. Information is promoted through the central Canberra Business website and regular e-newsletters.

In 2021, the ACT established and funded the Canberra Cyber Hub with the principal objective to advance the cyber ecosystem in Canberra, this includes uplifting the capability of SMEs.

The Canberra Cyber Hub does this by raising cyber literacy and awareness of non-cyber businesses through stepped programs starting with basic hands-on introduction to cyber for business through to "ask an expert" sessions. This includes workshops in partnerships with industry associations or Canberra Institute of Technology (CIT) aimed at bespoke sector audiences (e.g. hairdressers). It also makes available web resources for non-cyber companies and utilises opportunities such as National Cyber Security Month to promote cyber-security concepts.

Diverse, minority, and vulnerable communities

Noting Australia's multicultural and multi-lingual population, consideration should be given to the development of multi-lingual advice to support non-English speaking community members. To assist with the uptake of this advice, governments should collaborate with, and provide information and resources for sharing to, established CALD community groups, where there are existing relationships, trust and rapport built with communities on an ongoing basis.

Other avenues of promotion may include radio (community or mainstream) and print media, which despite not being *cyber,* will help to reach individuals who may have a more limited access or literacy to, and thus increased vulnerability in, the digital world. Digital 'hubs' that consolidate advice are helpful to create a single source of truth, and supports increased awareness of and uptake of advice. Practical, action-oriented, easy to understand messaging that compliments existing guidance, and is accessible amongst existing service provision, will best support success.

Support for citizens and victims of identity crime

Protecting vulnerable cohorts – including young people and students - in their digital experiences is critical in addressing identity crime. Embedding clear, curriculum-based guidelines on how to report identity-related incidents, seek support, and access advice empowers young people to respond effectively. Including age-appropriate case studies on identity theft and cyber bullying further strengthens awareness, helping students understand the risks and consequences of online actions and fostering a culture of digital responsibility.

Non-for-profit (NFP) sector considerations

Many NFPs provide services to the most vulnerable citizens in the community, which means they may hold a vast amount of personal sensitive information. It is important to support NFPs to protect citizen

identity and the sensitive information they hold and ensure that personal information and data is only retained under reasonable 'need to know' grounds.

NFPs face unique cybersecurity challenges due to limited resources, competing priorities with service delivery, and staff often lacking formal training. High turnover of volunteer-staff, varied resourcing and skill level, and offboarding practices that miss security considerations may lead to inconsistent cyber security practices and increased vulnerability. Cybersecurity may be deprioritised in favour of service delivery, which contributes additional barriers to embedding a strong security awareness and culture.

Horizon 2 presents an opportunity to reframe cybersecurity as a core investment in public trust rather than a 'nice-to-have' feature. Breaches can erode confidence and threaten funding, and so positioning cybersecurity as essential to organisational integrity may help bolster proactive cyber security measures.

Government support can play a vital role in embedding cyber security into everyday business practices, including by subsidising cyber upskilling, simplifying access to insurance, and offering tailored, low-cost tools. This may include targeted awareness for ransomware risks, phishing, and restoration planning. Aligning cybersecurity efforts with broader NFP goals, such as through peer learning and industry engagement, could also boost uptake and resilience.

Cyber insurance

Cyber insurance products are generally not considered affordable or accessible for small entities. Peak business bodies in the ACT have raised concerns about cost, complexity, and a lack of clarity around coverage and liabilities. Many SMEs face competing priorities, making cyber insurance appear secondary to immediate operational needs. Additionally, technical jargon and limited awareness of risks - such as ransomware, phishing, and restoration planning - may further hinder uptake.

Recommendations:

- That the Commonwealth build a consistent and targeted cyber awareness campaign; adopt a single national cyber brand; produce white-labelled, open-source content; and expand multilingual and culturally outreach programs.
- That the Commonwealth develop a national cyber literacy curriculum, with interactive modules for schools, teachers, and parents.
- That the Commonwealth prioritise cyber security awareness and resilience uplift for SMEs and NFPs, including through the provision of low or no-cost baseline cyber security standards that are practical and accessible.
- That the Commonwealth support the uptake of emerging AI technology with guidance, and uplift knowledge of cyber security and responsible and safe use of AI across the economy.

3.2 Shield 2: Safe technology

Supporting end-users to be informed on cyber security

The ACT welcomes an expansion of the national cyber awareness campaigns, particularly to CALD and minority communities. By introducing tailored education programs at both primary and secondary school levels, Australia can build early awareness and literacy around cyber security threats and strategies. This approach embeds cyber security within a broader 'essential skills' framework, making it accessible to all students, and not just those with a specialised interest in the field.

Safe technology in education

Incorporating education-specific use cases into the development of safe technology standards and certification processes would support all education jurisdictions. This is particularly important in relation to managing Bring Your Own Device (BYOD) programs in schools, where consistent, tailored standards can help ensure secure and effective technology use across diverse learning environments.

Foreign ownership, control or influence (FOCI) risks

By enhancing transparency on high-risk products, consumers and end-users can make more informed purchasing decisions to protect information. This is particularly true when considering FOCI risks and ICT purchasing and procurement decisions at both the personal or institutional level.

To support the ACT to manage the FOCI risks and supply chain risks associated with technology vendors, increased data sharing of assessments (within the appropriate security classification parameters) under the Technology Vendor Review Framework (TVRF) would provide early visibility across all levels of government.

Data access and transfer across the economy

To achieve this, the Commonwealth may consider embedding national standards to empower business, particularly SMEs, to plan and implement appropriate governance, processes, systems to gather, use, store and share data safely and securely beyond organisational boundaries. This could be further enhanced by implementing scaling criteria to certify entities in the whole-of-economy data ecosystem.

Furthermore, expansion of networks like the TISN to cover sectors outside of critical infrastructure, such as retail or hospitality, can support collaboration and up-skill diverse sectors in cyber security and trusted data sharing. Awareness campaigns exploring 'security culture' and 'need to know' information sharing practices may further support this objective.

Guidance for safe and responsible uptake for critical and emerging technologies

Among the complex national security risks should be consideration of the misuse of AI for misinformation and disinformation; increasingly scalable and far-reaching cyber threats; the exploitation of critical infrastructure vulnerabilities; and increased public distrust of opaque technology use and information security.

To support the safe uptake of critical and emerging technologies, the Commonwealth should provide clear, adaptable guidance that reflects national security priorities and community needs. A key design principle here should be *reusability*, with cyber awareness materials being designed for easy rebranding and reuse by States/Territories and other sectors. Targeted cyber awareness campaign should be inclusive and consider CALD, remote and minority groups in our diverse communities.

Recommendations:

- That the Commonwealth increase data sharing of FOCI assessments under the Technology Vendor Review Framework (TVRF) to provide early visibility across all levels of government, within the appropriate security classification parameters.
- That the Commonwealth consider the expansion of networks like the TISN to cover sectors outside of critical infrastructure.
- That the Commonwealth support the safe uptake of critical and emerging technologies, such as AI, with the provision of clear, adaptable guidance that reflects national security priorities and community needs.

3.3 Shield 3: World-class threat sharing and blocking

Threat sharing ecosystem

The ACT would welcome an update on the outcomes of the Health Cyber Sharing Network Pilot, aimed at accelerating sharing threat information and analysis at the sector-level. Insights into the efficacy of the program, and broad consultation after outcomes are identified, will help to inform selection of further pilots and programs at the national and sub-national level.

Roles and responsibilities in crisis

The ACT is comfortable with the current operational arrangements that outline the responsibilities of government relating to cyber security in a conflict or crisis scenario. To develop a more proactive posture, the ACT would welcome more exercising and cyber 'red teaming' exercises run by industry and government. Utilising these opportunities to share lessons learned across various stakeholders would assist to inform future programs.

Vulnerability disclosure program

The ACT broadly support the concept of a vulnerability disclosure program; however, further consideration is needed on how information is shared between levels of government and industry.

Recommendations:

- That the Commonwealth support cyber-security exercising that involves both industry and governments.

3.4 Shield 4: Protected critical infrastructure

The all-hazards risk management enshrined in the *Security of Critical Infrastructure Act 2018* (Cth; SOCI Act) is vital to the security of critical infrastructure for the way it provides a comprehensive framework for identifying, mitigating and responding to a wide variety of risks in an increasingly complex threat environment. The recent launch of the *ACT Critical Infrastructure Framework* demonstrates the ACT's commitment to advocate the benefit of all-hazards risk management approach to manage our critical government services.

Regulation of the private sector and efforts to uplift security standards do not occur in isolation - they operate within a broader regulatory framework involving government, legislation, and national priorities. To effectively promote enhanced Australian Government security requirements, this must be a coordinated national effort, not only a bilateral undertaking between the Commonwealth and the private sector. A national approach that is co-designed with sub-national governments is essential to ensure regulatory alignment and consistent implementation across jurisdictions. At the same time, sector-specific regulations that are developed in consultation with relevant partners help ensure that obligations are proportionate to risk, clearly understood, and practically enforceable, supporting both compliance and improved security outcomes.

In the submission on the *Cyber Security Legislative Reforms Consultation Paper*, the ACT highlighted that the regulatory burden of recent reforms to the SOCI Act have yet to be assessed and evaluated to determine the successes and impediments to industry uplift and the consequential positive impacts to Australia. The increased burden on critical infrastructure assets under the SOCI Act, particularly the related financial impacts, must be considered as part of any assessment seeking to determine if the

current regulatory landscape appropriate balances addressing risks, and mandating preventative and remediating responses that asset owners are genuinely capable of meeting.

The ACT further highlighted the potential for reforms to offer uneven protections, leaving similarly sensitive data outside critical infrastructure vulnerable. Importantly, regulation can be most effective when considered alongside broader initiatives under the *Cyber Security Strategy*, such as Systems of Government Significance and recent cyber legislation, which may provide additional mechanisms to achieve the objectives of the SOCI Act.

Recommendations:

- That the Commonwealth evaluate outcomes under the SOCI Act against the Regulatory Impact Assessment, in close consultation with State/Territory governments and critical infrastructure sectors.
- That further consideration be given to the potential for inconsistent application on data sets and systems of national importance that could result in significant community, government or business disruption if compromised.
- That future development of critical infrastructure regulation be co-designed with State/Territory governments.

3.5 Shield 5: Sovereign capabilities

Cyber workforce

To identify and prioritise sovereign capabilities for growth, early and meaningful engagement across jurisdictions is critical. This ensures that capability development is informed by local needs, leverages regional strengths, and aligns with national security and economic objectives. This supports a coordinated, inclusive, and future-ready cyber ecosystem.

Governments have a key responsibility in promoting a sustainable and diverse cyber workforce and business ecosystem. The development of Australia's cyber workforce and ecosystem must be treated as a national endeavour, with sub-national governments engaged as strategic partners, and not only as stakeholders alongside industry, given the vastly different roles and capabilities.

Developing the cyber workforce begins with education. Embedding Cyber Security as a core curriculum subject in schools will help cultivate a larger pool of talent with foundational knowledge and interest in the field. Additionally, encouraging female participation in STEM subjects at the school level is essential to fostering diversity and increasing representation in tertiary education and vocational training, ultimately strengthening the future cyber workforce.

Furthermore, the overall development of the cyber workforce should take a holistic approach that considers transferrable skills, work experience, and longer-term retention of expertise in cyber security. It should also consider how retention can be sustained in the sector to reduce the risk of burnout or attrition to competing areas of the economy.

Workforce Development and Migration

The ACT undertakes work in several areas to support a sustainable and diverse cyber workforce and local cyber business ecosystem. This includes leveraging the National Skills Agreement, a five-year strategy aimed at strengthening the workforce in critical and emerging industries - including cyber security and encouraging uptake of the Free TAFE initiative funded by the ACT and Australian Governments. The program will continue through to 2026, offering 600 places per semester at the CIT.

In consultation with industry and the CIT, the ACT has included cyber qualifications in the Fee-Free TAFE initiative, which has seen strong uptake. Cyber Security has emerged as one of the most in-demand areas, with the Certificate IV in Cyber Security becoming the most popular course, attracting 264 enrolments in 2023 alone.

The initiative has been particularly successful in supporting:

- Young people (17–24 years)
- Jobseekers
- Women in non-traditional fields
- People with disability, and
- Veterans and unpaid carers.

Short courses such as Introduction to Cyber Security Awareness and Organisational Cyber Security are also available, providing accessible entry points into the digital workforce.

The ACT's approach is guided by an *Industry Action Plan* including advanced technology, which encompasses cyber security. Developed in close consultation with industry and training providers, the plans outline over 100 actions to attract and grow the local workforce.

A key component is the expansion of the *ACT Skilled Capital* program, which provided Registered Training Organisations (RTOs) with over 600 new subsidised training places across a range of industries in 2024-25. Among these is the *Certificate IV in Cyber Security*. This qualification is designed to equip students with practical skills to meet the growing demand for cyber professionals in Canberra.

Additionally, the Canberra Cyber Hub plays a central role in developing a skilled cyber workforce.

- It works to demystify cyber careers, build understanding of the diversity of roles in the sector, and identify workforce pipelines and skills requirements.
- Through targeted communications - via social media, newsletters, and its website - the Hub promotes education offerings and career pathways, showcasing Canberra cyber businesses as skills-first employers.
- A key initiative is the annual *Cyber Career Symposium,* which raises awareness of career pathways and educational opportunities for school leavers, tertiary students, and career transitioners. This includes hands-on cyber experiences and direct engagement with industry.
- Collaboration with CIT ensures that vocational pathways remain aligned with industry needs, offering accessible entry points such as short courses and the *popular Certificate IV in Cyber Security*. CIT's practical training complements these outreach efforts, helping to build a pipeline of job-ready professionals.
- The Hub also works closely with UNSW Canberra, providing industry perspective and support for the Work Integrated Learning. This partnership helps scope opportunities and connect students with industry partners, ensuring that academic learning is matched with real-world experience.

Together, CIT, UNSW Canberra, and the Canberra Cyber Hub form a collaborative ecosystem that supports lifelong learning, career mobility, and the development of a resilient cyber workforce in the ACT.

Migration

Through the *ACT Nominated Skilled Migration* program, the ACT nominates a range of IT and cyber occupations to empower ACT businesses and citizens to become more resilient to cyber incidents. Specifically, this includes IT Business and Systems Analysts, Software and Application Programmers, IT

Security Specialists, and Computer Network Professionals - all of which are listed on the *ACT's Critical Skills List*. These occupations reflect the growing demand for cyber expertise across sectors. In the 2024–25 migration program year, 8 per cent of ACT nominations were made to migrants with these four nominated occupations, out of a total of 150 eligible occupations.

Business ecosystem development

Canberra's compact city and unique knowledge economy enables connections between tertiary and research institutions, advanced technology businesses and government.

A foundation of ACT's innovation ecosystem is the *Canberra Innovation Network* (CBRIN), supported by the ACT Government. It brings together key tertiary institutions including Australian National University, University of Canberra, UNSW Canberra and CIT, and is focused on connecting innovation and entrepreneurship with science and research. CBRIN provides a forum for research and business and investment to jointly consider challenges and devise solutions.

More specifically the Canberra Cyber Hub supports the development of the cyber security ecosystem and connections with other advanced technology sectors. The Canberra Cyber Hub's program of activities provides opportunities for cyber businesses to expand their client base, uplifts ecosystem capability through providing access to training and information relating to market readiness and business strategy and shares industry intelligence, opportunities, and information. It also seeks to provide insights to government and others about issues of importance to the cyber sector.

Sovereign capabilities for growth and development

The ACT, through the Canberra Cyber Hub supports the development of local cyber-security businesses to contribute to Australia's sovereign capabilities. Further analysis is required for the development of broader policy ideas to address how sovereign capabilities are best identified and priorities. Key sovereign capabilities of interest would include quantum, artificial intelligence, cellular, and low earth orbit satellite technology.

The Australian Government can further support the development of sovereign capabilities through accessible procurement opportunities to local SMEs, particularly to Defence.

Recommendations:

- That the Commonwealth continue to provide funding support that strengthens the workforce in critical and emerging industries such as Free TAFE initiative and other initiatives.
- That the Commonwealth further support the development of sovereign capabilities through accessible procurement opportunities to local SMEs, particularly to defence-related industries.

3.6 Shield 6: Strong region and global leadership

Nil response.

Summary of consultation paper questions

Part 1 - Developing our vision for Horizon 2

#	Question	Our Response
2.1 Outlook for Horizon 2		
1	What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?	Page 6
2.2 Collaborating across all levels of Australian Government		
2	Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?	Pages 6-7
2.3 Monitoring progress in a changing world – a conceptual framework for evaluating cyber security outcomes		
3	Does the high-level Model resonate, and do you have any suggestions for its refinement?	Page 7
4	Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?	Page 7

Part 2 – Shield-level focus for Horizon 2

#	Question	Our Response
3.1 Shield 1: Strong businesses and citizens		
5	What could government to do better target and consolidate its cyber awareness message?	Pages 7-10
6	What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?	Pages 7-10
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.)?	Pages 7-10
8	How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?	Pages 7-10

9	What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's?	No response.
10	What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?	Pages 7-10
11	Do you consider cyber insurance products to be affordable and accessible, particularly for small entities? If not, what factors are holding back uptake of cyber insurance?	Pages 7-10
12	How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?	No response.
13	How could the government further support businesses and individuals to protect themselves from ransomware attacks?	No response.
14	Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?	No response.
15	How can support services for victims of identity crime be designed to be more effective in the context of increasing demand?	Page 9
16	Which regulations do you consider most important in reducing overall cyber risk in Australia?	No response.
17	Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?	No response.
3.2 Shield 2: Safe technology		
18	What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?	No response.
19	How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?	Pages 10-11

20	What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?	Page 11
21	How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?	Page 11
22	Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How does Government and Industry work together to achieve this aim in an evolving global threat environment?	Pages 10-11
23	What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies?	Page 11
3.3 Shield 3: World-class threat sharing and blocking		
24	What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?	Page 12
25	Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry? Does the government need to provide clarity on permissible and non-permissible Active Cyber Defence in the Australian context? **Discrepancy between Policy Discussion Paper and Consultation Questions Paper*	No response.
26	How could government further support industry to block threats at scale?	No response.
27	How could the use of safe browsing and deceptive warning pages be amplified?	No response.
28	What more is needed to support a thriving threat sharing ecosystem in Australia? Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?	Page 12

29	How can we better align and operationalise intelligence sharing for cyber security and scams prevention?	No response.
30	Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?	Page 12
31	How could government better incentivise businesses to adopt vulnerability disclosure policies?	No response.
32	Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?	Page 12
3.4 Shield 4: Protected critical infrastructure		
33	How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?	Pages 12-13
34	Are there significant cyber security risks that are not adequately addressed under the current framework?	No response.
35	Is the regulatory burden on industry proportionate to the risk and outcomes being sought?	No response.
36	What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?	No response.
37	How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?	Pages 12-13
38	How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?	No response.
3.5 Shield 5: Sovereign capabilities		
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?	Pages 13-15

40	What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?	Pages 13-15
41	What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?	No response.
42	How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals?	Pages 13-15
43	How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities?	No response.
44	How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?	Page 15
45	What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?	Pages 13-15
3.6 Shield 6: Strong region and global leadership		
46	Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?	No response.
47	Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?	No response.
48	Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?	No response.
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?	No response.

50	What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?	No response.