FUTURE SKILLS ORGANISATION
Finance Technology Business

Horizon 2

2023-2030 Australian Cyber Security Strategy

9 September 2025

JSC
Jobs and Skills Council
Finance, Technology and Business
An Australian Government Initiative

Contents

Introduction

Future Skills Organisation (FSO) welcomes the opportunity to respond to the *Charting New Horizons – Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy Policy Discussion Paper* (the discussion paper).

FSO is one of ten Jobs and Skills Councils (JSC) funded by the Australian Government, with a strong focus on skills. FSO's mission is to advance transferable and industry-specific skills in the finance, technology, and business (FTB) sectors. Through close collaboration with industry, unions, and governments, under tripartisanship, and with the training and education sector, we work collectively to benefit employers, employees, and those seeking to enter finance, technology or business (FTB) sectors.

Development of Australia's cyber workforce has been occurring, at least, for a decade. However, multiple cyber skill shortages remain, with many directly tied to architecture, testing, and operations, affecting job roles such as cyber security architect, penetration tester, cyber security engineer, cyber security operations coordinator, cyber security analyst, and cyber governance, risk, and compliance specialists. In particular, system architecture and cyber security have been forecast to have some of the largest skills gaps in tech by 2030 underscoring continued demand for these functions.

Reasons for these shortages are many and varied.

While cyber workforce development was boosted by the ASD Cyber Skills Framework (2020), which defined roles, capabilities, and skills proficiencies essential to cyber, the Framework lacks scalability as it is not easily applied to smaller organisations, who are unlikely to have a dedicated cyber person let alone a cyber team. An alternative approach to assist organisations to identify the capabilities required as part of a 'layered defence in depth' would be helpful.

Insufficient numbers of employers are currently providing earn while you learn (EWYL) and other entry level opportunities to the cyber workforce, especially with sufficient scale and sustainability to have material impact on these critical skills shortages.

Pathways into technology careers, including for cyber security, are not clearly defined or visualised and, accordingly, not well communicated to current and future job seekers. All of which limits participation rates and interest in cyber education and skills training during and beyond schooling that also hinders cyber qualification design and development.

This issue is exacerbated by the need for an uplift in cyber security literacy in schools and in identifying and educating towards those career pathways, including by increasing participation in science, technology, engineering, and mathematics (STEM) subjects.

Finally, industry have recognised the need for a set of interconnected skills to operate in the cyber workforce including across Artificial Intelligence (AI), cyber security, and generalist skills (such as planning and organising, digital engagement, initiative and innovation, adaptability, teamwork, and emotional intelligence).

Our recommendations and submission consider these issues in further detail, with specific reference to questions 6, 39, 40 and 41 in addition to related policy issues.

Question 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*?**

It is encouraged that there be an uplift in cyber security literacy in schools and in educating towards career pathways for developing cyber talent pipelines, such as increasing diversity in science, technology, engineering, and mathematics (STEM), as two distinct objectives. It appears many schools don't mandate basic cyber awareness training, which at the fundamental level is needed for good online hygiene irrespective of career needs. Further, it would be worthwhile to see schools offering opportunities through courses that expose students to potential cyber careers.

Recommendation 1

Pathways into technology careers, including for cyber security, to be clearer and visually communicated more effectively to lift participation in cyber education and skills training during K-12 and post-secondary school.

FSO is undertaking a range of work in the vocational education and training (VET) sector for impact in cyber:

- **Updating the Information and Communications Technology (ICT) Training Package**, through training product development, with new and updated urgent training products for specialist cyber security. The aim is to provide a Certificate IV in Cyber Security, and to deliver further cyber security training products at other Australian Qualification Framework (AQF) levels.[1]
- **Entry level pathways** work designed to be a skills-led analysis of how new entrants may identify VET pathways to employment in the cyber domain, amongst other domains.[2]
- **Uplift Digital Capability** in response to urgent and growing need for digital capability skills across the Australian economy. This work involves the design of units of competency (UoCs) to define essential digital skills and, through collaboration with delivery partners, the development of training resources, based on DigComp 2.2. The final accredited products will be housed within the BSB Training Package for cross-industry use. This uplift in digital capability has three components:
  - Digital capability
  - Generalist artificial intelligence
  - Generalist cyber security[3]

[1] https://www.futureskillsorganisation.com.au/project-specialist-cyber-security-skills/

[2] https://www.futureskillsorganisation.com.au/project-entry-level-pathways/

[3] https://www.futureskillsorganisation.com.au/project-uplift-digital-capability/

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?

It is worth noting development of Australia's cyber workforce has been occurring, at least, for a decade. This cyber workforce development was boosted by the ASD Cyber Skills Framework (2020)[4], which defined roles, capabilities, and skills proficiencies essential to cyber. This was accompanied by a significant funding commitment in the Cyber Security Skills Partnership Innovation Fund, part of Australia's Cyber Security Strategy 2020, Cyber Security National Workforce Growth Program.[5] While a step forward with what is a good framework, it lacks scalability as it is not easily applied to smaller organisations, who are unlikely to have a dedicated cyber person let alone a cyber team.

It is necessary to understand and apply lessons learnt over the past 5–10 years, such as the above examples, with both government and industry collaborating in communicating and implementing these lessons.

A further understanding is to complement the existing compliance approach, and existing skills frameworks such as the Skills Framework for the Information Age (SFIA)[6], with a culture and risk management approach. For example, in terms of culture, by communicating what government and industry collectively see as to what capabilities organisations should embed as part of a 'layered defence in depth' approach to cyber security.

Recommendation 2

To support life-long learning, with clear pathways from education and training into work, including to support cyber skills, and to support movement across a harmonised tertiary education sector, the Government should consider:

- Accelerating the development and promotion of a national skills taxonomy for the cyber workforce, by pointing to common skills frameworks already adopted by industry, employers, the government sector, and education and training institutes, such as the Information Age (SFIA) and the Digital Competence Framework for Citizens.[7]
- Supporting adoption of skills-first hiring and training for cyber roles by providing national leadership and examples of implementation within the federal, state and territory public sectors.
- Providing free practical skills assessments, such as provided by SkillsAware,[8] to support the recognition of existing skills held by both the domestic and migrant workers and those seeking to enter the cyber workforce, both for specialist and for generalist skills.[9]

[4] https://www.asd.gov.au/sites/default/files/2022-10/ASD-Cyber-Skills-Framework-v2.pdf

[5] https://business.gov.au/grants-and-programs/cyber-security-skills-partnership-innovation-fund

[6] https://sfia-online.org/en

[7] https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp_en

[8] https://skillsaware.com/

[9] Nature Human Behaviour | Volume 9 | April 2025 | 673–687 *Skill dependencies uncover nested human capital* page 680 https://www.nature.com/articles/s41562-024-02093-2; and The Treasury, 2023, *White Paper on Jobs and Opportunities*, page 87, https://treasury.gov.au/sites/default/files/2023-09/p2023-447996-07-ch5.pdf

- Supporting greater alignment and targeted funding of cyber training across the states and territories under the National Skills Agreement (NSA),[10] given one of the seven initial national priorities set out in the NSA is *ensuring Australia's digital and technology capability*.
- Recognising the greatest demand is for generalist cyber skills across all roles rather than specialist roles, therefore generalist cyber skilling should be prioritised. That is, as noted in FSO's Uplift Digital Capability activity, in response to urgent and growing need for digital capability skills across the Australian economy, there is a need for generalist cyber skills given cyber security is everyone's business.
- Promoting and recognising organisations that genuinely commit to the 20 percent pledge for cyber roles, through hiring 20 percent of their workforce via alternative pathways by 2030 (per the NSW Digital Skills and Workforce Compact).[11]

Question 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?

Facilitating career transitions via upskilling or short courses, such as VET skill sets, and attracting under-represented groups, such as women in tech, are crucial to filling skills shortages.

As a successful initiative, awarded funding through the AustCyber Projects Fund in 2019, TAFEcyber[12] aims to support the development of Australia's cyber security training capabilities. The TAFE consortium provides students with the most needed technical skills and knowledge to gain a sustainable and growing career in cyber security.

TAFEcyber priorities are supported by key government and industry partners including the Australian Cyber Security Centre (ACSC), which forms part of the Australian Government Australian Signals Directorate (ASD). TAFE consortium members provide a range of cyber security qualifications.

Recommendation 3

Centres of Excellence models, such as TAFEcyber, should be expanded to include VET, higher education, and schools in recognition of the value of these models when partnered with industry, especially where these arrangements promote a diverse range of industry role models to potential new entrants.

[10] https://federalfinancialrelations.gov.au/agreements/national-agreement-skills clause A28 (f) page 7.
[11] https://www.nsw.gov.au/education-and-training/nsw-digital-compact/20-per-cent-alternative-pathways-pledge
[12] https://www.tafecyber.com.au/

The Institute of Applied Technology Digital (IAT-D), see case study at Attachment A, provides a solid base and learning for a Centre of Excellence model. IAT-D programs for underrepresented groups in cyber security also warrant examination.

A key barrier is insufficient numbers of employers providing opportunities and with sufficient scale and sustainability to have material impact on critical skills shortages. Even in the case of CyberCX, where they are using industry led, non-accredited training, it relied in-part on government grants to initiate funding of the program, noting CyberCX contributed the same value in-kind to start the Academy (and has continued to operate the Academy post exhaustion of that grant funding). That is, government funding is critical to drive these programs.

Question 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?

FSO's interest lies in broadening the pipeline by drawing workers with adjacent skills into tech and cyber roles. Workforce data compiled by FSO identifies where tech skills lie in the economy (many in non-tech sectors) and underscores the opportunity to retrain those workers for cyber roles.

If seeking to attract workers from other industries it is likely that generalist skills will most facilitate that transfer, combined with opportunities for industry supported Earn While You Learn (EWYL) programs that equip workers with the needed specialist skills (see below for further information on EWYL models).

Further, people need to see role models like them in the cyber workforce to attract them to the cyber workforce.

Recommendation 4

A starting point is to think about the generalist skills needed to participate in Australia's cyber workforce and to promote diverse role models with these skills.

Cyber, AI, Quantum and Digital Skills Convergence

FSO notes that many of the most acute cyber skills shortages are concentrated in specialist skill areas such as architecture, testing, and operations. Roles experiencing significant demand include cyber security architect, penetration tester, cyber security engineer, cyber operations coordinator, cyber security analyst, and cyber governance, risk and compliance (GRC) specialist. System architecture and cyber security are projected to have among the largest specialist skills gaps by 2030, underscoring the urgency of building capacity in these functions.

However, cyber skill shortages cannot be considered in isolation from broader technology capabilities. Increasingly, Artificial Intelligence (AI) and digital capability are deeply interconnected with cyber, forming part of the emerging "new tech talent equation." [13] [14]

[13] https://www.futureskillsorganisation.com.au/workforce-plans/workforce-plan-2025/
[14] https://s3b.au/

For example, in the finance sector, more than 60 per cent of firms plan to scale AI adoption, making integrated AI–cyber skills a priority for managing sector-specific risks and compliance. Both global and domestic regulatory settings highlight the need for combined expertise in areas such as digital forensics, resilience testing, and secure financial architecture. [15]

Governance-related cyber roles, including legal, policy, risk, and compliance, are also growing in importance. As AI becomes central to operations, and as privacy, regulatory, and assurance requirements intensify, these occupations will be pivotal in ensuring secure, ethical, and resilient adoption of new technologies.

Recommendation 5

Greater coordination across government is required to ensure that approaches to digital skills development (including AI and Cyber Security) are complementary to one another and consider all digital skills holistically.

FSO Skills Accelerator-AI

In July 2025 the FSO launched the *FSO Skills Accelerator-AI* in partnership with industry, educators and trainers as a collaborative approach to co-design AI training and share resources.[16]

With a goal to reach learners and more than 30,000 VET educators and administrators, through the *FSO Skills Accelerator-AI* the FSO is seeking to drive a new benchmark for nationwide AI capability. The integration of AI training into national standards will empower Australians to keep pace and prosper in an AI-driven future.

With Microsoft as a founding partner, and alongside other supporting organisations, the aims to support VET teachers, trainers, administrators and learners to build essential AI capabilities as a foundation for a faster, more connected, and forward-looking skilling system.

The *FSO Skills Accelerator-AI* will support the training product development activity FSO has commenced to update ICT training package with new and urgent training products related to the skills needed to work with specialist AI to provide recommendations for the direction of the Specialist AI training products. Likely outputs of this work include specialist Artificial Intelligence Training products and the potential development or refinement of units of competency in other AI areas identified as essential or urgent.[17]

Generalist Skills for Cyber Professionals

Employers consistently emphasise the importance of generalist skills, such as planning and organising, digital engagement, initiative and innovation, adaptability, teamwork, and emotional intelligence, alongside specialist technical skills, including cyber-specific

[15] Standards such as: https://www.bis.org/basel_framework/ ; https://www.ifrs.org/groups/international-sustainability-standards-board/; and those imposed domestically such as through the Australian Prudential Regulation Authority and the Australian Securities & Investments Commission.

[16] https://www.futureskillsorganisation.com.au/skills-accelerator-ai/

[17] https://www.futureskillsorganisation.com.au/project-specialist-ai/

expertise. This reflects the emerging “new tech talent equation” of AI, cyber and human skills.

The importance of generalist skills in cyber has the potential to reduce gender bias in STEM pathways, as these skills are valued on par with technical or specialist competencies. Strong generalist skills further enhance workforce mobility, enabling learners and workers to move fluidly within and across industries as labour market needs evolve.

As the Australian and global economies undergo structural transformation, driven by industry convergence, rapid technological change, and evolving job roles, workers increasingly require transferable, cross-industry skills to succeed. This shift is recognised in the Australian Government’s *White Paper on Jobs and Opportunities*, which notes:

> ‘Human capital accumulation requires an investment in people to build up not just technical skills and knowledge but also the core transferable skills needed to be resilient and adaptable through structural change.’[18]

Recommendation 6

In recognition of the importance of generalist skills, initiatives that undertake a skills-first approach to supporting mobility for adjacent professionals to move into cyber should be considered.

Earn While You Learn Models

FSO recently undertook work to consider how to strengthen EWYL models, including traineeships, degree apprenticeships and non-accredited programs, to close the skills gap and boost workforce participation.[19] This work identified five challenge areas to improve the scalability and sustainability of EWYL models that may inform cyber EWYL models:

- *Increase awareness and engagement*. Many employers lack understanding of VET and traineeship pathways, often viewing them as less valuable than university qualifications. This results in low employer participation.
- *Strengthen funding mechanisms*. Fluctuating funding and the reduction of key subsidies have made it harder to promote traineeships and attract employer involvement.
- *Make qualifications more attractive*. Current qualifications often do not match employer needs, leading to a preference for non-accredited or higher education solutions.
- *Simplify the system*. The complexity of the traineeship system makes it difficult for employers to navigate, discouraging their participation.
- *Develop and trial new EWYL models*. Even among leading ICT employers, few earn while you learn programs have achieved significant scale or long-term sustainability – a new approach is required.

[18] The Treasury, 2023, *White Paper on Jobs and Opportunities*, page 87, https://treasury.gov.au/sites/default/files/2023-09/p2023-447996-07-ch5.pdf

[19] https://www.futureskillsorganisation.com.au/developing-the-tech-workforce-unlocking-the-potential-of-earn-while-you-learn/

Examples of industry models trialled or piloted for cyber include:

- Cyber Academy, a pilot that included Deloitte, TAFE NSW, Swinburne University of Technology, and the University of Wollongong, provided school leavers with a pathway into cyber via a three-year EWYL model. The pilot had strong student interest, with 75 students commencing, but it was challenging to attract employers at scale, without subsidies to help cover employment costs of the traineeship, so the targeted 400 new entrants is currently limited to 75 students.
- The Australian Training Company (ATC) Catholic Diocese IT Traineeships in New South Wales, has been running successfully for 20 years, with graduating students being potential entrants for the cyber workforce.

Other examples included at Attachment A are TAFE Queensland's Cyber Traineeship, CyberCX Academy, and even the Victorian Digital Jobs Program.

The FSO proof of concept work for its entry level pathways project involved significant stakeholder consultation with recruiters, managers and cyber experts. The consultation supported the view mid-career transitions, for example from nursing, law, physical security, and sales, are viable and valuable. Further, military veterans and first responders are ideal for these roles if supported as career changers.

Targeted programs supporting these transitions, such as bootcamps, microcredentials, and mentorships, are effective, as are organisations such as With You With Me[20] that bridge previous professional experience with formal qualifications to smooth transitions to job readiness.

Where governments may need to incentivise is with employers to prioritise entry level roles, work integrated learning opportunities and EWYL models to widen the funnel of participation. Case studies repeatedly point to the fact that subsidised training is insufficient, and employers require financial incentives to de-risk hiring entry talent.

For clear pathways from education and training into work, the Government should consider:

- Supporting subsidies to employers to make cyber EWYL more attractive in hiring decisions.
- Providing national leadership in implementing EWYL models that are underpinned by more modular and stackable training and includes relevant Industry Certifications, such as for post graduate EWYL models.

Recommendation 7

Consideration be given to the Department of Home Affairs and the Apprenticeships and Digital Projects Group with the Department of Employment and Workplace Relations collaborating on seeking to include cyber as an apprenticeship or traineeship on the Australian Apprenticeship Priority List.

[20] https://withyouwithme.com/

Entry Level Pathways

Beyond training to support smooth career transitions, a critical requirement is better alignment between cyber workforce demand and supply. This includes accessible tools such as visualised career pathways based on skills, "day in the life" role profiles, representation of people currently in these roles ("people like me"), and transparent information on the frequency, location, and availability of entry-level jobs. Such information helps confirm the reality of opportunities for prospective workers.

Clearer cyber career pathways can also guide curriculum and qualification design. Entry-level pathways represent clusters of related jobs that share overlapping knowledge and skill requirements. As such, they can inform, and be supported by, an education approach defined by agreed learning outcomes across schooling and post-school systems. These outcomes, while meeting broader educational goals, should be shaped by a collective understanding of the generalist and digital skills required for employer-defined roles.

Importantly, FSO is undertaking work to identify and map up to ten entry-level pathways into technology roles, with a focus on high-demand skill areas.[21] This work will draw on recognised capability and skills frameworks, such as DigComp 2.2[22] and the Skills Framework for the Information Age (SFIA),[23] and will involve consultation with learners, industry, and training providers throughout the mapping process.

Recommendation 8

Consideration be given to mapping and visualisation of cyber entry level pathways to inform a common understanding of the skills required for entry into cyber job roles.

Conclusion

This submission identifies several interconnected challenges to developing the cyber workforce, including the need to strengthen cyber security literacy in schools, enable skills transfer from other industries, expand Earn While You Learn models, and improve the mapping of entry-level pathways.

Addressing these priorities in a coordinated manner will be essential to building a resilient and sustainable cyber workforce.

[21] https://futureskillsorganisation.com.au/project-entry-level-pathways/

[22] JRC Publications Repository - DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes

[23] https://sfia-online.org/en

Attachment A

Earn While You Learn (EWYL) Cyber Case Studies

Key insights:

1. Subsidised training is not enough, and employers need subsidies to engage in these programs
2. Hybrid offerings like Cyber Academy offer promise but require significant investment to both structure the program, project manage it and attract employers.
3. All programs, regardless of the type of training have required government investment.
4. Sustainability and scale are going to require coordinated effort from state and federal governments to support the streamlining of experiences for employers.
5. Efforts by the FSO to update qualifications and increase the modularity and stack-ability of accredited training will support efforts to use training to upskill diverse cohorts including career changers, school leavers and underrepresented groups.

Victorian Digital Jobs Program (VDJP) - Victoria

Section	Summary
Overview	Launched in July 2021 to build a new digital talent pipeline during COVID border closures. Short, industry-aligned training followed by paid work placements. Delivered through multiple providers across core digital specialisations.
Model at a glance	**Target cohort:** People 30+ with 10+ years' experience, COVID-impacted workers, regional Victorians, women returning to work. **Length**: 24 weeks. **Credential**: Short course then placement. **Delivery**: Blended (face to face and online), with career support during training. **Employer model:** Government-brokered placements, with an initial $5,000 host incentive.
Funding and employer model	Initial $64m; FY 2024-25 $4.4m for 400 places. Employers pay placement wages.
Scale and outcomes	5,000+ trained; ~85% completion across first nine rounds. 1,000+ paid placements; ~80% stayed with their host beyond 12 weeks.
Diversity and inclusion	59% women; 63% multilingual participants.
Strengths	Fast scale; strong diversity results; centralised attraction, screening and matching.
Challenges and risks	Employer placements remain the constraint; variable provider quality; mentoring and evaluation need resourcing.

Australian Training Company - Catholic Diocese IT Traineeships - New South Wales

Section	Summary
Overview	Long-running program with Catholic Education NSW. Clear pathway from Certificate III to Certificate IV. Roles focus on implementing IT solutions in schools.
Model at a glance	**Length**: 12-24 months. **Delivery**: Face-to-face block training 8-9 days each school holiday. High performers may add Microsoft or Cisco Academy certification. Runs only in NSW; Queensland expansion stalled due to policy and funding settings.
Funding and employer model	Training funded via Smart and Skilled; ATC passes incentives to hosts. Removal of incentives reduces employer uptake. School budgets are fixed, so cost rises resulted in the number of places cut.
Scale and outcomes	35 Certificate III starters and 35 Certificate IV graduates each year. 90%+ completion, ~70% are employed in industry within 3 months, ~20% proceed to university, ~30% take roles within the Dioceses.
Diversity and inclusion	5% women; 20% learners with disability; likely under-reporting of neurodivergence cohort.
Strengths	Block delivery aligns with school terms. Close employer partnership informs electives. Pre-traineeship enterprise skills and graduate mentors boost readiness and retention.
Challenges and risks	Trainer shortages for ATC's RTO. Fixed school budgets constrained places, Interstate expansion is hampered by policy and funding.

CyberCX Academy - National

Section	Summary
Overview	Employer-delivered program launched July 2022 to grow a sovereign cyber workforce at scale. Three intakes each year.
Model at a glance	**Length**: 26 weeks. **Delivery**: 4 weeks fundamentals, 5 weeks skills, 5 weeks practice placement, 12 weeks client work. Associates start work in week 10 in pods of 5-7 or embedded in delivery teams. Part-time option Mon-Thu in major cities.
Funding and employer model	$3m start-up grant. Single-employer model (CyberCX). Paid throughout training and work phases. Permanent contract on completion. Pod projects billed at a lower blended day rate during training.

Scale and outcomes	~320 commencements; 80-90% retention; ~80% utilization by 9 months; >90% remain with CyberCX after training. 31:1 applications to places.
Diversity and inclusion	45% women; all-female cohort launched November 2024. A part-time option was also run for flexibility for those working,
Strengths	Tight integration of training and client work. Clear employment pathway. Multi-stream curriculum aligned to market needs.
Challenges and risks	High delivery and wage costs without grant support. Scale limited by single-employer model. Risk of talent poaching.

Cyber Academy (TAFE NSW, UOW, Swinburne) - New South Wales and Victoria

Section	Summary
Overview	Multi-partner pathway using the traineeship system so employers can hire while students study. Links Diploma of IT (Cyber) to a Bachelor of IT with credit.
Model at a glance	**Length:** 3 years. **Delivery:** 2 days study and 3 days paid work weekly. VET and higher education delivered concurrently to complete both in 3 years. **Employers**: Include government and industry.
Funding and employer model	Employers cover wages (about $40,000 plus on-costs). Cyber Academy facilitation is about $5,000 per student, initially covered by a $500,000 NSW grant. Students exit with about $20,000 HELP debt.
Scale and outcomes	75 starts; 92% continuing; 48 Diploma completions to date.
Diversity and inclusion	38% women; 5% regional. Neurodiversity is not measured for privacy reasons.
Strengths	Integrated pathway with work-integrated assessment. Strong governance across government, industry and education.
Challenges and risks	No formal off-ramp or partial VET exit. Employer demand below plan. Salary level limits appeal for older candidates.

TAFE Queensland Certificate IV in Cyber Security Traineeships - Queensland

Section	Summary
Overview	Commenced 2023. Co-designed with industry. Priority status took two years to secure. Direct-hire model without a GTO; SMEs predominate.
Model at a glance	Certificate IV in Cyber Security. **Delivery:** First 8-9 units online; remaining units on secure TAFE sites. One day per week on campus plus short blocks. Flexible by region and employer need.
Funding and employer model	The government covers training costs. Employers pay wages with a floor of about $50,000 per year. User Choice co-contribution $1.60 per nominal hour, covered for the initial 60 places. Optional support via ACAPs.
Scale and outcomes	60 places funded; 20 employment contracts issued. ~1,000 learners complete Certificate IV Cyber outside traineeships via Fee-Free TAFE.
Diversity and inclusion	Predominantly male cohort.
Strengths	Flexible delivery: Online start lowers barriers; Security Operations Centre (SOC) facilities support applied learning.
Challenges and risks	Trainer shortages. Large employers did not follow through on placements, with reliance on SMEs with limited supervision. Lack of regional access to secure facilities. Removal of federal incentives and competition from Fee-Free TAFE reduce employer appetite. The matching process needs strengthening.

Institute of Applied Technology – Digital (IATD) – Sydney

Section	Summary
Overview	Launched in early 2023 as part of NSW investment in applied technology institutes. Programs co-designed with TAFE NSW, Macquarie University, UTS and Microsoft. Focus on cyber security, AI, cloud, data and software. Delivery uses a cyber range and the AnyTown simulation environment.
Model at a glance	**Target cohort:** general public, women, regional learners, Aboriginal and Torres Strait Islander people, neurodivergent learners (priority cyber scholarships). **Length:** microskills about 5 hours; microcredentials 6-8 weeks. **Credential:** digital badge for microskills; recognised microcredential stackable into higher qualifications.

	Delivery: self-paced online plus facilitated online and face to face. **Employer model:** co-design with Microsoft and university/TAFE partners; workplace-relevant environments such as a cyber range.
Funding and employer model	NSW funded capital over $125m to establish facilities and funded operations of about $100m across the four-year pilot for IAT-D and IAT-Construction. A $2.35m Commonwealth grant funded 100 cyber microcredential scholarships targeting underrepresented cohorts. Microcredentials priced at about $260 (foundation) and about $510 (intermediate); microskills typically free. Industry partners contribute expertise and facilities; NSW funds core infrastructure.
Scale and outcomes	100,000+ enrolments across microskills and microcredentials since 2023. Female participation above 40% overall. 38,000+ SMEs engaged in microskills. Specialist infrastructure established: cyber range and AnyTown simulated city.
Diversity and inclusion	300+ cyber scholarships targeted to women, Aboriginal and Torres Strait Islander peoples, neurodivergent learners and regional participants. Partnerships with Akkodis, Microsoft and AWSN to create new pathways for women into cyber. Scholarship cohorts recorded 50%+ women, well above the estimated 17-25% in the cyber workforce.
Strengths	Large-scale uptake in a short timeframe. Gender outcomes stronger than broader ICT benchmarks. Industry-backed co-design keeps content current. Immersive facilities enable practice-based learning.
Challenges and risks	Sustain completion rates in microcredentials, not just microskills. Build clearer pathways from microskills and microcredentials into jobs or higher qualifications. Ongoing reliance on government and partner funding for scholarships and facilities.

Future Skills Organisation

futureskillsorganisation.com.au

PO Box 16194, Collins Street West,
Melbourne VIC 8007

The Future Skills Organisation is a Jobs and Skills Council funded by the Australian Government Department of Employment and Workplace Relations.