PRELIMINARIES

1. This implementation plan is made between the Commonwealth of Australia (Commonwealth) and the Australian Capital Territory (ACT) under the 2024–2028 National Skills Agreement (the NSA) and should be read in conjunction with the NSA and the NSA Bilateral Implementation Plan Guidance.

2. Once executed, this implementation plan and any updates agreed with the Commonwealth, will be appended to the NSA and will be published on the Commonwealth's Federal Financial Relations website (https://federalfinancialrelations.gov.au).

3. This implementation plan is expected to expire on 31 December 2028 (in line with the NSA), or on completion of the initiative, including final performance reporting and processing of final payments against milestones.

4. In all public materials relating to the policy initiatives, the ACT will acknowledge the Commonwealth's contribution with the following statement: the Cyber Security TAFE Centre of Excellence is a joint initiative between the Australian Government and the ACT Government.

REPORTING AND PAYMENTS

Reporting

1. Performance reporting will be due by 31 March and 30 September each year until the cessation of this Agreement, or the final payment is processed.

2. The ACT will provide to the Commonwealth a traffic light status and activity summary on all policy initiatives.

3. The Commonwealth will provide templates for the purposes of reporting.

Payments

1. The Commonwealth will make payment subject to performance reporting demonstrating the relevant milestone has been met.

2. As part of the performance reporting, the ACT will provide evidence of what has been delivered in the reporting period. Payments will be processed once performance reports have been assessed and accepted.

3. Where a payment is due at a reporting period (31 March and/or 30 September), the ACT will complete the relevant section of the reporting template and provide the evidence required as agreed in the Milestones and Payments associated with this Implementation Plan.

TAFE CENTRES OF EXCELLENCE (Clause A112 to A116 of the NSA)

Cyber Security TAFE Centre of Excellence (Cyber Security TCoE***)***

1) Outline and priority area(s) addressed:

According to the Future Skills Organisation (FSO), Australia could face a shortfall of more than 370,000 digital professionals by 2026. With a 60 per cent increase in reported cybercrime since 2020,[1] the nation urgently needs highly skilled cyber security professionals. Despite high demand, many graduates require further on-the-job training to meet stringent national digital infrastructure requirements. The skills gap is compounded by a lack of diversity in the workforce.

To bolster Australia's sovereign capabilities, the Canberra Institute of Technology (CIT) Cyber Security TAFE Centre of Excellence (Cyber Security TCoE) will focus on developing and enhancing cyber skills essential to national security and will support the implementation of the 2023-2030 Australian Cyber Security Strategy. In partnership with the Canberra Cyber Hub, Future Skills Organisation and University of New South Wales Canberra (UNSW Canberra), the Cyber Security TCoE will collaborate with businesses, students, research organisations and tertiary education providers to address critical skills gaps and build the national workforce to safeguard Australia's digital future. Based at the new CIT Woden campus in Canberra, the Cyber Security TCoE will attract $5.0 million in matched funding under the National Skills Agreement.

Canberra is recognised as Australia's cyber security capital – a hub where advanced high-tech companies and national security organisations converge to protect our nation's critical infrastructure. Canberra is home to a number of intelligence agencies, defence primes and broader government sector, for which demand for these skills continues to increase. The Canberra Cyber Hub, supported by the ACT Government, connects industry, education providers and talent to drive cyber resilience, including through national networks.

Establishing a Cyber Security TCoE in the ACT will leverage this robust ecosystem to address skills shortages, increase participation of underrepresented groups, enhance graduates' job readiness, strengthen the pipeline of skilled workers and accelerate innovation to respond to the rapid emergence of new digital technologies and threats affecting Australian government agencies and businesses.

2) Functions and activities of the TAFE Centre of Excellence:

The Cyber Security TCoE will bolster Australia's sovereign capabilities and resilience by enhancing the cyber readiness of businesses and government agencies, while developing a robust pipeline of skilled professionals to address critical workforce shortage.

Key Cyber Security TCoE activities will include:

- establishing a national hub for TAFEs, facilitating professional learning opportunities for educators, and opportunities to co-design innovative and future-focused education and training products, incorporating essential enterprise skills and capabilities
- establishing an incubator hub and applied research program in collaboration with industry and tertiary institutions, with a national focus on cyber threats, prevention and security
- exploring cyber readiness in energy, utilities and critical infrastructure to strengthen Australia's sovereign capability, including collaboration with the Electric Vehicle TAFE Centre of Excellence to identify cyber risks in electric vehicles
- developing tailored cyber courses mapped to a range of learner cohorts and emerging skills gaps across the nation, including initiatives for senior secondary students, cross-sector workers and final-year trades students aspiring to become small business owners

[1] ACS Digital pulse 2024

- developing postgraduate microcredentials aimed at university graduates from multiple industries to create pathways into the cyber sector
- developing a cyber higher apprenticeship program in partnership with UNSW Canberra
- scaling the successful pilot between CIT and the Canberra Cyber Hub to develop work placement opportunities and ensure job-ready graduates
- working with government agencies, industry and business to bolster cyber literacy across the workforce.

A comprehensive stakeholder engagement strategy and robust governance framework will be established to oversee partnership activities, projects and program milestones. A Program Steering Committee will provide executive oversight of the Cyber Security TCoE's work, while specialised working groups—developed in collaboration with the Electric Vehicle TAFE Centre of Excellence—will focus on key areas such as applied research, learning design, priority cohorts and partnerships. A Stakeholder Steering Group will provide advice, share insights and inform project decisions, drawing members from industry, universities, unions and peak bodies.

Annual work plans will define program schedules and activities, with progress reports provided for each reporting period. Insights and leading practice will be shared through the TAFE Cyber Consortium, an educator network facilitated by TAFE Directors Australia and the broader National TAFE Network.

3) Partnerships and engagement:

The Cyber Security TCoE will build on a foundation of robust stakeholder engagement and nationally significant strategic partnerships. In collaboration with the Canberra Cyber Hub, the Cyber Security TCoE will act as a vital nexus connecting cyber businesses with its work program, ensuring industry, government organisations and peak bodies continuously inform its progress. Extensive stakeholder research conducted by CIT has already yielded valuable insights, highlighting clear benefits for employers, students and the Australian cyber sector across all proposed project streams.

Leveraging established relationships with the Canberra Cyber Hub, Future Skills Organisation, UNSW Canberra and the TAFE Cyber Consortium, the Cyber Security TCoE will cultivate a network of organisations dedicated to national skills development and workforce enhancement. Pilot programs will be trialled, monitored and refined before a broader rollout to TAFEs across Australia. The Cyber Security TCoE will harness expertise within the national TAFE cyber network, and collaborate with both TAFE institutions and universities, to develop innovative curricula, career pathways, applied research initiatives and higher apprenticeship programs.

Given the cyber industry predominantly employs university graduates, a significant focus will be on integrating the tertiary sector by creating seamless pathways between VET and higher education. The partnership with UNSW Canberra will explore development of a degree/higher apprenticeship program that combines advanced cyber knowledge with practical work experience. Additionally, cyber skills microcredentials will be introduced for graduates from ICT and related fields who are seeking to upskill, reskill or transition into the cyber workforce.

The Cyber Security TCoE will work with the Canberra Cyber Hub to promote career and education pathways, including options for school leavers, to enhance visibility of career options and training opportunities. The approach will foster diversity and inclusion, partnering with industry and specialist community organisationsto develop pilot programs that improve employment outcomes for underrepresented groups such as women, neurodiverse individuals and Aboriginal and Torres Strait Islander peoples. These programs will examine barriers to participation and success, build on existing wrap-around support services, and pilot targeted in-class assistance to boost retention and completion rates.

A dedicated Aboriginal and Torres Strait Islander pilot program will be developed in collaboration with CIT Yurauna, the institute's Aboriginal and Torres Strait Islander Educational Centre of Excellence. Yurauna provides study support, cultural guidance, community activities and tailored courses. An Indigenous-led, culturally appropriate introduction to the cyber industry will be designed, including essential work skills training such as resume writing and interview preparation.

As a founding partner of the Canberra Innovation Network, CIT will leverage its expertise and industry exposure to advance the Cyber Security TCoE work program. By collaborating closely with both the Canberra Cyber Hub and the Canberra Innovation Network, the Cyber Security TCoE will foster development of collaborative programs and applied research projects. In particular, the Canberra Innovation Network will play a key role in developing the Cyber Incubator Hub program, providing students with opportunities to engage in applied research projects alongside local entrepreneurs, universities and industry organisations.

The Cyber Security TCoE will work with the National TAFE Network once established to drive excellence in teaching and learning and best practice in skills development by TAFEs. This will be a critical collaboration for the Cyber Security TCoE and the ACT commits to the Cyber Security TCoE to operating in such a way that it:

- plays a national leadership role with employers, unions, universities, Jobs and Skills Councils, and other relevant stakeholders to identify, develop and deliver education and training solutions that meet industry needs across Australia, and
- partners with TAFEs and other public providers across Australia to assist them with non-financial support to build their capability and capacity to deliver responsive skills training for industries.

The ACT recognises the mutual benefits of collaboration between the VET and higher education sectors and commits the Cyber Security TCoE to developing partnerships to support and deliver on its objectives, including with universities, Jobs and Skills Councils (JSCs), employers and unions. These partnerships could take different forms, and are likely to evolve over time, but could include:

- university representation in the Cyber Security TCoE's governance structures
- exchanging expertise and experience in the design and delivery of education and training relevant to the Cyber Security TCoE's governance, including higher apprenticeship pathways
- establishing credit recognition arrangements and entry pathways between VET and higher education for education and training relevant to the Cyber Security TCoE, and/or
- facilitating joint opportunities for applied research relevant to the Cyber Security TCoE.

The ACT acknowledges that there is the potential for duplication of effort between the Cyber Security TCoE and relevant JSCs. The ACT is committed to working with the Commonwealth to maximise the collective benefit for the skills and training system through the Cyber Security TCoE, and commits to early and regular engagement with relevant JSCs on all the Cyber Security TCoE's activities for the purposes of:

- minimising the potential for duplication of effort
- sharing learnings on best practice and support knowledge translation, and
- partnering on projects of mutual interest where appropriate.

The Cyber Security TCoE will support and partner with other TAFEs across Australia (including dual-sector universities), including through the National TAFE Network (once established), to build capability, share curriculum and best-practice, and improve teaching and learning outcomes.

Commonwealth Investment ($)	State Investment ($)	Planned Start Date	Planned End Date
$2.5 million	$2.5 million	1 August 2025	31 December 2028

TAFE Centre of Excellence – approach to matched funding arrangements (clause A114 refers) – to be reconciled over the life of the NSA.

Details of matched funding	2025-26	2026-27	2027-28	2028-29	Total
ACT Contribution	$700,000	$500,000	$750,000	$550,000	$2,500,000
Commonwealth Contribution	$700,000	$500,000	$750,000	$550,000	$2,500,000
Total	$1,400,000	$1,000,000	$1,500,000	$1,100,000	$5,000,000

The ACT Government will provide details of their matched funding contributions at the end of each financial year, commencing 1 July 2025 until 31 December 2028. Final payments under this implementation plan may be reduced where the total contribution by the ACT Government over the life of the project does not align with the Commonwealth contribution.

Performance Indicators

CIT will develop a reporting framework to track performance. In addition, the Cyber Security TCoE will provide six-monthly progress and expenditure reports to monitor establishment and ongoing operations against defined milestones. Once operational, the Cyber Security TCoE's annual report will be structured around the following indicators.

Quantitative indicators:

- pilot programs – the number of pilot programs introduced to support priority cohorts.
- student enrolments – the number of new enrolments in both accredited and non-accredited training programs, with specific reporting for priority cohorts (e.g., women, Aboriginal and Torres Strait Islander peoples, neurodiverse individuals) to assess the impact of tailored supports
- student completions: pre- and post-establishment completion rates for accredited and non-accredited training, evaluating the effectiveness of implemented support measures, the relevance of skills and knowledge provided and the efficiency of pathways and transitions
- industry placements – data on industry placements for graduates to assess the relevance and transferability of the skills and knowledge delivered
- applied research projects – the number of applied research projects initiated and completed, providing an indicator of collaboration between government entities and other stakeholders
- stakeholder engagement – the rate of stakeholder engagement and the number of partnerships formed, measuring how well industry is integrated with education and training delivery.

Qualitative indicators:

- networking and engagement – a summary of networking and engagement activities with stakeholders, including other TAFE Centres of Excellence, along with an assessment of the benefits these activities provide in fostering collaboration with government and other stakeholders
- training product development – an analysis of new training product development, encompassing initial explorations of training needs and skills gaps, industry collaboration, training and assessment strategies, and any intended accreditation pathways
- higher apprenticeship development – progress on developing a higher apprenticeship program, indicating contributions toward creating effective pathways and transitions.

• student engagement – feedback from student engagement surveys to evaluate the quality of training, education and support provided • feedback on school engagement – insights from student feedback on school engagement initiatives and perceptions of cyber courses • job outcomes – case studies documenting job outcomes for graduated students.

Evaluation arrangements

August 2025 - March 2026	Develop a comprehensive evaluation plan that integrates key quantitative and qualitative reporting indicators to assess the impact of Cyber Security TCoE measures on achieving the outcomes defined in the Theory of Change. This plan will establish robust data collection mechanisms to ensure that all necessary data—including baseline information—is gathered to support both interim and final evaluations.
31 March 2027 Interim findings	An interim evaluation of the Cyber Security TCoE will be conducted. In alignment with the outcomes defined in the Theory of Change, the evaluation will cover the following components: • efficiency and effectiveness of the support measures • participation and job outcomes for target groups • participation, completion rates and job placements to determine the quality and relevance of training • degree/higher apprenticeship development • Cyber Security TCoE engagement with cyber educators nation-wide • stakeholder feedback. Insights gleaned from the interim evaluation will inform refinements to the Cyber Security TCoE's measures and will be shared with the National TAFE Network.
31 December 2028 Final evaluation	At the conclusion of the Cyber Security TCoE program, a final evaluation will be conducted using a methodology similar to the interim evaluation, with additional focus on the following areas: • degree/higher apprenticeship impact • industry feedback • applied research outcomes.

MILESTONES AND PAYMENTS – TAFE CENTRES OF EXCELLENCE

Milestone	Evidence	Payment Value Up To (Commonwealth funded)	Commonwealth reporting period
Milestone 1: Initial payment on agreement of bilateral implementation plan	Bilateral implementation plan agreed with Commonwealth	$250,000	31 July 2025
Milestone 2. Commonwealth acceptance that the ACT has established the Cyber Security TAFE Centre of Excellence, to be demonstrated by: • development of a Project Plan for the Cyber Security TAFE Centre of Excellence that specifies the deliverables to be achieved and associated timeframes • stakeholder engagement and partnership development strategies (including employers, unions, universities, JSCs and other TAFEs), and • a Cyber Security TAFE Centre of Excellence governance framework.	Report signed by ACT senior official with responsibility for skills that outlines key activities of the Cyber Security TAFE Centre of Excellence in the reporting period to 30 September 2025 that includes or attaches: • a Project Plan with timeframes and deliverables for key Cyber Security TAFE Centre of Excellence activities over the life of the NSA until December 2028 • a Stakeholder Engagement Strategy, and • a Cyber Security TAFE Centre of Excellence Governance Framework	$250,000	30 September 2025
Milestone 3. Commonwealth acceptance that the ACT has continued to operate the Cyber Security TAFE Centre of Excellence, to be demonstrated by: • recruitment activities • governance groups established • stakeholder engagement and partnerships development activities, (including	Report signed by ACT senior official with responsibility for skills that outlines key activities of the Cyber Security TAFE Centre of Excellence in the reporting period to 31 March 2026 that includes or attaches: • an updated Project Plan with timeframes and deliverables for key Cyber Security TAFE Centre of Excellence activities over the life of the NSA until December 2028 • a Recruitment Report and Organisational Chart • Terms of Reference for governance groups	$200,000	31 March 2026

employers, unions, universities, JSCs and other TAFEs) • a draft outline of Aboriginal and Torres Strait Islander Pilot project in collaboration with CIT Yurauna, and • the development and / or delivery of cyber training.	• details of stakeholder engagement and strategic partnership activities • a draft Aboriginal and Torres Strait Islander Project Outline – including detail on any partnerships or consultations to date, and • details of the development and / or delivery of cyber training (including tailored cyber courses, postgraduate microcredentials, and the cyber higher apprenticeship program).		
Milestone 4. Commonwealth acceptance that the ACT has continued to operate the Cyber Security TAFE Centre of Excellence, to be demonstrated by: • stakeholder engagement and partnerships development activities, (including employers, unions, universities, JSCs and other TAFEs), and • the development and / or delivery of cyber training.	Report signed by ACT senior official with responsibility for skills that outlines key activities of the Cyber Security TAFE Centre of Excellence in the reporting period to 30 September 2026 that includes or attaches: • an updated Project Plan with timeframes and deliverables for key Cyber Security TAFE Centre of Excellence activities over the life of the NSA until December 2028 • details of stakeholder engagement and strategic partnership activities, and • details of the development and / or delivery of cyber training (including tailored cyber courses, postgraduate microcredentials, and the cyber higher apprenticeship program).	$200,000	30 September 2026
Milestone 5. Commonwealth acceptance that the ACT has continued to operate the Cyber Security TAFE Centre of Excellence, to be demonstrated by: • stakeholder engagement and partnerships development activities, (including employers, unions, universities, JSCs and other TAFEs) • the development and / or delivery of cyber training, and	Report signed by ACT senior official with responsibility for skills that outlines key activities of the Cyber Security TAFE Centre of Excellence in the reporting period to 31 March 2027 that includes or attaches: • an updated Project Plan with timeframes and deliverables for key Cyber Security TAFE Centre of Excellence activities over the life of the NSA until December 2028 • details of stakeholder engagement and strategic partnership activities, and • details of the development and / or delivery of cyber training (including tailored cyber courses, postgraduate	$300,000	31 March 2027

• the commencement of applied research projects.	microcredentials, and the cyber higher apprenticeship program), and • an Applied Research Scoping Framework, and details of applied research activities.		
Milestone 6. Commonwealth acceptance that the ACT has continued to operate the Cyber Security TAFE Centre of Excellence, to be demonstrated by: • stakeholder engagement and partnerships development activities, (including employers, unions, universities, JSCs and other TAFEs) • the development and / or delivery of cyber training, and • the continuation of applied research projects.	Report signed by ACT senior official with responsibility for skills that outlines key activities of the Cyber Security TAFE Centre of Excellence in the reporting period to 30 September 2027 that includes or attaches: • an updated Project Plan with timeframes and deliverables for key Cyber Security TAFE Centre of Excellence activities over the life of the NSA until December 2028 • details of stakeholder engagement and strategic partnership activities, and • details of the development and / or delivery of cyber training (including tailored cyber courses, postgraduate microcredentials, and the cyber higher apprenticeship program), and • details of applied research activities.	$450,000	30 September 2027
Milestone 7. Commonwealth acceptance that the ACT has continued to operate the Cyber Security TAFE Centre of Excellence, to be demonstrated by: • stakeholder engagement and partnerships development activities, (including employers, unions, universities, JSCs and other TAFEs) • the development and / or delivery of cyber training, and • the continuation of applied research projects.	Report signed by ACT senior official with responsibility for skills that outlines key activities of the Cyber Security TAFE Centre of Excellence in the reporting period to 31 March 2028 that includes or attaches: • an updated Project Plan with timeframes and deliverables for key Cyber Security TAFE Centre of Excellence activities over the life of the NSA until December 2028 • details of stakeholder engagement and strategic partnership activities, and • details of the development and / or delivery of cyber training (including tailored cyber courses, postgraduate microcredentials, and the cyber higher apprenticeship program), and • details of applied research activities.	$300,000	31 March 2028

Milestone 8. Commonwealth acceptance that the ACT has continued to operate the Cyber Security TAFE Centre of Excellence, to be demonstrated by: • stakeholder engagement and partnerships development activities, (including employers, unions, universities, JSCs and other TAFEs) • the development and / or delivery of cyber training, and • the continuation of applied research projects.	Report signed by ACT senior official with responsibility for skills that outlines key activities of the Cyber Security TAFE Centre of Excellence in the reporting period to 30 September 2028 that includes or attaches: • an updated Project Plan with timeframes and deliverables for key Cyber Security TAFE Centre of Excellence activities over the life of the NSA until December 2028 • details of stakeholder engagement and strategic partnership activities, and • details of the development and / or delivery of cyber training (including tailored cyber courses, postgraduate microcredentials, and the cyber higher apprenticeship program), and • details of applied research activities.	$250,000	30 September 2028
Milestone 9: Commonwealth acceptance that the ACT has continued to operate the Cyber Security TAFE Centre of Excellence, to be demonstrated by: • stakeholder engagement and partnerships development activities, (including employers, unions, universities, JSCs and other TAFEs) • the development and / or delivery of cyber training • the continuation of applied research projects, and • completion of final outcomes and evaluation report.	Report signed by ACT senior official with responsibility for skills that outlines key activities of the Cyber Security TAFE Centre of Excellence in the reporting period to 31 December 2028 that includes or attaches: • an updated Project Plan with timeframes and deliverables for key Cyber Security TAFE Centre of Excellence activities over the life of the NSA until December 2028 • details of stakeholder engagement and strategic partnership activities, and • details of the development and / or delivery of cyber training (including tailored cyber courses, postgraduate microcredentials, and the cyber higher apprenticeship program), and • details of applied research activities, and • final outcomes and evaluation report.	$300,000	31 December 2028
	Total	**$2,500,000**	

The Parties have confirmed their commitment to this implementation plan as follows:

Signed *for and on behalf of the Commonwealth of Australia by*

The Honourable Andrew Giles MP
Minister for Skills and Training
24 / 7 /

Signed *for and on behalf of the Australian Capital Territory by*

Michael Pettersson MLA
Minister for Skills, Training and Industrial Relations
1 / 7 /2025