Powering Australia's technology brilliance

acs.org.au

ACS Submission to Horizon 2 of the Australian Cyber Security Strategy 2023-2030 Discussion Paper

29 August 2025

29 August 2025

Assistant Secretary
Cyber Policy & Programs
Cyber and Infrastructure Security Centre
Department of Home Affairs
Canberra, ACT

Dear Assistant Secretary,

As the peak body for Australia's IT profession, ACS acknowledges the Department's leadership in developing the Australian Cyber Security Strategy 2023-2030 and its importance in ensuring a secure digital environment for all Australians.

ACS welcomed the Horizon 1 focus on professionalising the cyber security workforce and will continue to support the government's work on helping grow and maintain Australia's cyber security workforce.

Australia will need 54,000 more people skilled in cyber security operations and management by the end of the decade to combat the increasing frequency and sophistication of attacks. Currently, there is a shortage of entry-level roles in cyber, with most existing roles requiring prior experience in software development[1].

Many factors limiting the growth of the cyber security workforce also affect the broader IT profession. ACS believes that the cyber workforce would benefit from efforts to improve the mobility and development of Australian IT professionals and digital skills more generally, including through:

- Greater promotion and use of internationally recognised digital skills frameworks like SFIA
- A skills recognition and attainment system that is modular and stackable
- Allowing more entry level tech roles through earn-while-you-learn models (including traineeships and apprenticeships)
- Helping the training system meet industry demand for vendor and other industry-specific certifications.

This submission was developed in collaboration with the ACS Cyber Security Committee[2] which comprises a coalition of seasoned professionals, thought leaders, and experts working in cyber security across the economy. Feel free to contact me by [redacted]

Yours faithfully,

[redacted]

[redacted]

[redacted]

Australian Computer Society

About ACS

For nearly 60 years, ACS has represented Australia's world-class technologists as the peak body for the IT profession. ACS sets and upholds professional standards – including a code of ethics – and plays a central role in guiding the development of the cyber security profession in Australia.

ACS is an Accredited Partner of the Skills Framework for the Information Age (SFIA), enabling consistent digital skills assessment and workforce planning across industry, government, and education.

ACS is a signatory to the Seoul Accord[3] which sees it accredit Australian university IT degrees against standards recognised under the Accord. This accreditation ensures Australian IT-related degree programs meet international academic standards for preparing graduates to enter the profession.

ACS is the relevant skills assessing authority for IT-related occupations under the instrument authorised by Migration Regulations 1994[4]. In this role, ACS assesses whether an applicant's qualifications and employment experience meet the standards for the nominated OSCA (formerly ANZSCO) occupation. The Department of Home Affairs uses that assessment to determine whether the applicant meets the skills requirement of their nominated visa.

ACS has been a regular contributor to consultation on changes to OSCA, including advocacy in favour of the dedicated cyber security occupations[5] that are now a feature of both the classification and the Core Skills Occupation List.

While ACS is extremely proud of its critical role in ensuring Australia's migration and higher education systems produce quality IT professionals, ACS is proudest of its 40,000 constituent members who operate, develop, and maintain the IT systems that keep Australia running.

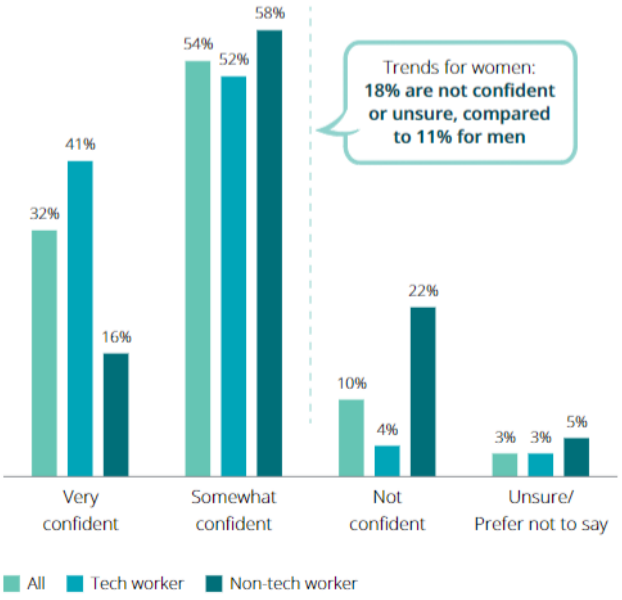
Digital technologies are inarguably the most important enabling feature of our nation's prosperity with the tech sector contributing an estimated $134 billion to Australia's economy in the 2024 financial year. This could not happen without dedicated, highly skilled IT professionals.

Cyber Skills are Digital Skills

There were 137,500 cyber security professionals employed in Australia in 2024, yet 54,000 additional cyber professionals will be required to meet demand and mitigate the effects of cyberattacks by 2030. Those additional professionals include 28,000 core technology workers (such as cybersecurity engineers and penetration testers) and 27,000 cyber-dedicated workers (such as cyber compliance specialists and chief information officers). In total, 84% of occupations have skills that will be affected by cybersecurity by 2030 and 18% of all worktime will be affected.[6]

The workforce shortage especially is acute in domains such as system design and implementation, information security as well as cloud security, cyber threat intelligence and malware analysis. Many of the skills needed for the cyber domain are not cyber specific, either. Understanding how networks are configured, how IT systems are designed, how secure code works, authentication principles, and how cloud solutions are integrated are crucial generalist IT skills.

Intuitively, IT professionals will thus be more adept at moving into and supporting the cyber security workforce than non-technical professionals. However, it is increasingly important for workers across all industries to understand, identify and report cybersecurity risks. Almost one-third of non-tech workers report low confidence levels when it comes to recognising and appropriately responding to cyber threats (27%). Confidence levels are lower among women, with 18% of women selecting not confident or unsure compared to 11% for men.[7]



Source: Deloitte workforce survey (2025)

A general uplift of Australia's tech skills will produce cyber security dividends. Many of the problems that limit the cyber security workforce are faced by much of the IT profession, including:

- lack of entry level roles
- mismatch between what job ads ask for (degrees) and what industry wants (experience, vendor certs)
- limited use of common language to describe skills and capabilities.

Answers to Discussion Questions

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?

Setting the Digital Skills Standard

As a buyer of IT products and services – and direct employer of tech workers – the government has a significant role in affecting positive change for the cyber workforce, and IT profession in general.

The government can set a standard by continuing to use and promote the Skills Framework for the Information Age (SFIA) which provides a consistent, globally recognised description of workplace capabilities and role-specific skills. The Australian Public Service Commission (APSC) and the Digital Transformation Agency (DTA) already rely on SFIA for digital workforce development. The APS Digital Traineeship Program aims to create employment opportunities for underrepresented groups while referencing SFIA to leverage industry lead micro-credentials and earn-while-you-learn programs.[8]

SFIA helps organisations use a skills-based approach to workforce development and planning that is becoming more common in industry. According to recruitment firm Hays, 86% of hiring managers say they are adopting skills-based hiring practices to better address talent shortages.[9] This is about trying to measure and understand what a candidate can actually do, rather than looking mostly at their formal qualifications and job titles. Part of a skills-based approach to hiring involves re-writing job descriptions to capture expected capabilities.

Capability is a more holistic way of viewing professional skills, knowledge, and experience as a set of interrelated qualities. One common capability model distinguishes between professional/technical skills (like the ability to write code), general workplace skills, behaviours (like soft skills), experience, and knowledge. In this view, qualifications and certifications are ways of demonstrating that a worker has one or many aspects of capability.

The capability view recognises that skills and experience can be gained outside formal training, like by taking on new work responsibilities or contributing to community projects. This is also commonly referred to as recognition of prior learning (RPL). For the many alternative pathways into tech jobs, this shift in thinking is crucial if we are to give Australia's workforce the kind of flexibility that can adapt to sudden market changes, like those caused by AI.

Jobs and Skills Australia is currently developing a National Skills Taxonomy to establish a unified framework for defining and categorising skills across the Australian workforce. ACS thinks this work should be fast-tracked with a digital skills pilot that is interoperable with SFIA.

Supporting the Local Ecosystem Through Procurement

Around the world, nations are increasingly approaching the technology sector as a strategic capability, using procurement as a fundamental lever to drive sovereign growth and act as a core enabler of adjacent industries. Totalling $8.3 billion in 2023-24, Commonwealth ICT procurement "will have exceeded the funding for the National Reconstruction Fund and in four years it will be more than the Future Made in Australia program"[10].

When ICT services are delivered by Australian-based workers – including apprentices and early-career professionals – more of each procurement dollar stays in the local economy, supporting domestic capability and reducing reliance on offshore service delivery. This is particularly important in cyber security, where sovereign capability and local talent pipelines are critical to national security. There is a need for government to continue recognising and leaning on the broader benefits of procuring from Australian suppliers.[11]

One key lever in procurement already exists to help develop local talent. DEWR's Skills Guarantee mandates that Commonwealth IT procurements valued at $10 million or more include a set portion of labour hours allocated to apprentices, trainees, IT cadets, and – under an enhanced Version 1.2 due to commence in October 2025 – 'Learning Workers'. This policy also has incremental targets for women as part of a drive for inclusion and workforce development.

The Skills Guarantee's full effect depends on two enabling conditions. All parties – government, suppliers, training providers – must share a common language for describing and measuring skills. Embedding SFIA into the National Skills Taxonomy will take a model that already exists and expand it to the rest of the economy.

There must also be fit-for-purpose pathways to fill the roles created under the Skills Guarantee. This means modernising the ICT Training Package to embed stackable micro-credentials, formally recognise vendor certifications, and strengthen RP) – as ACS already does in its professional certification process. Combined with better-designed digital and cyber apprenticeships, these changes would give employers practical, credible options for meeting their Skills Guarantee commitments while delivering workers with industry-relevant capabilities from day one.

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?

ACS's independent, award winning tech news publication *Information Age* has published first-hand accounts of people who followed the standard advice for getting into cyber security – degrees, boot camps, capture the flags, online courses – only to struggle breaking into the industry.

Journalist Rohan Neagle described his frustration at needing "1-5 years' experience, with certs to boot" to apply for an entry-level position. "I arrived at the all-too-simple answer," he concluded. "The industry is desperate for workers, but it sure as hell is not desperate enough to train them."[12]

Small business owner Jane Rathbone had a similarly disheartening experience after completing an associate degree in cyber security.

"Certificate in hand, I gleefully visited employers across Melbourne, looking forward to starting the exciting new career I'd worked so hard to achieve," she said. "Sadly, I didn't receive the warm welcome I'd been expecting. A few actually laughed at me, though many were nicer, as they informed me that, no, they didn't have any entry-level roles."[13]

A dearth of entry level roles is the single point of failure for Australia's cyber security workforce. Earn-while-you-learn programs like apprenticeships and traineeships meet this gap by providing paid, structured on-the-job training while developing nationally recognised skills.

VET courses alone may not be sufficient as ICT-related VET programs have low completion rates with ICT ranked 8th out of 11 industries for completions.[14] But combined with on-the-job training in an earn-while-you-learn format, this helps overcome the entry barrier. ACS members have also expressed how cyber security apprenticeships – which have started through university programs or informal pathways – often result in ongoing employment.

The volume of cyber apprenticeships has been increasing in the United States, with NIST citing a 254% increase in the number of cyber security apprentices between 2018 and 2023.[15] Cyber apprenticeships have been growing in the UK, but the OECD notes that "absolute numbers remain relatively low – especially at the intermediate-level".[16]

Degree apprenticeships are a best practice model of industry training gaining popularity in the UK and Europe. These programs encourage employers to invest in the deep technical skills required to uplift Australia's ICT levels to meet demand. For example, the University of South Australia has begun a country-first trial of its Software Engineering Degree Apprenticeship program in which participants study an ACS-accredited Bachelor of Software Engineering (Honours) degree over five years while working in a paid position with an industry employer.[17]

To build a strong pipeline into cyber security and other high-demand ICT roles, Australia's VET system must deliver qualifications that reflect the pace and nature of change in the digital sector. This requires updating the ICT Training Package to:

- Embed stackable micro-credentials and vendor certifications (e.g., AWS, Azure, GCP, cloud-native security, CompTIA) so learners acquire job-ready skills recognised directly by employers. ACS already recognises vendor certifications as evidence during migration skills assessment.[18]
- Strengthen RPL so existing vendor certifications, short courses, and workplace experience count toward formal qualifications. ACS already applies this principle through its professional certification program for IT professionals, offering recognition of experience and industry credentials alongside formal qualifications.
- Ensure a fast refresh cycle so training package content can be updated in months rather than years, keeping pace with emerging technologies and threats.

This work is already underway through the Future Skills Organisation's ICT Training Package Update Project, which presents a unique opportunity to embed industry-alignment, stackability, and vendor credential recognition in a systemic way. The Horizon 2 Strategy's focus on a responsive, scalable cyber workforce depends on these reforms being supported and delivered at pace.

Incentivising Digital and Cyber Apprenticeships

Once ICT VET qualifications are modernised, they can underpin robust apprenticeships and traineeships in digital roles. But without stronger employer and learner incentives, uptake will remain low. Government ought to consider ways of incentivising employers to take on cyber apprentices, especially for small-to-

medium enterprises who need the in-house talent but haven't got the time or resources to take on the extra responsibilities of nurturing an apprentice without extra support.[19]

Currently, the Australian Apprenticeships Priority List (AAPL) only includes occupations in OSCA major groups 3 and 4, excluding most ICT roles – which are classified under major group 2 (Professionals) – from higher subsidies and supports.

To close this gap, the AAPL should be expanded to include high-demand professional occupations with apprenticeship or traineeship delivery models, starting with cyber security, cloud, and other critical ICT roles. International models, such as the UK's degree apprenticeship framework, show how professional-level apprenticeships can combine formal study with paid work to great effect in the ICT sector.

Expanding the AAPL's scope in this way would:

- Unlock employer incentives for hosting apprentices in digital roles
- Encourage alternative, earn-while-you-learn pathways into the ICT profession
- Direct public investment toward occupations that are critical to Australia's economic and national security, as set out in Horizon 2.

Investing in Mentorship

Mentoring is a proven way to support new entrants into the cyber workforce, yet most opportunities today are ad hoc and dependent on personal goodwill. ACS already delivers structured mentoring through its ACS Professional Year (PY) program which combines internship experience with a 13-week online mentoring and peer-support component, giving graduates targeted guidance as they transition into the workforce[20]. ACS branches also offer mentorship programs that match early-career ICT professionals with experienced mentors, and include structured activities, mentor coaching, and networking opportunities.

The challenge is reach and consistency. Currently, mentoring depends on branch capacity and local demand. A government-supported national cyber mentoring framework could scale these efforts across all states and territories, ensuring that every new entrant to the cyber workforce has access to structured, supported mentoring.

Such a framework could:

- Build on the proven ACS mentoring model already operating in branches
- Provide national coordination and resourcing to extend mentoring beyond branch boundaries, including online platforms for remote and regional participation
- Link mentoring formally to cyber apprenticeships, traineeships, and earn-while-you-learn pathways, ensuring every apprentice has access to both structured work experience and professional guidance
- Incentivise participation by recognising mentors with professional development credits (e.g., CPE hours) and providing modest support to SMEs to release staff time.

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?

A wide range of professional backgrounds can provide fertile ground for recruitment into cyber security roles. Transferable skills are the foundation of skills-based hiring and workforce development, and they are particularly relevant to cyber.

Professionals in compliance and risk (such as regulatory officers or risk evaluators) are well suited for governance, risk, and compliance (GRC) functions in cyber as they have experience in applying frameworks or standards to managing regulatory obligations. Because many cyber roles also involve elements of crisis response, workers with experience in high-stakes environments (such as air traffic controllers) are also a strong fit, offering composure under pressure, rapid decision-making, and attention to detail.

Australian Defence Force (ADF) personnel bring highly coveted qualities to cyber security roles, including active security clearance, which may reduce hiring friction for roles that require trustworthy access to sensitive systems. Rigorous training and operational environment cultivate transferable strengths like structured decision-making, adherence to protocols, resilience under pressure, teamwork, and leadership. Programs like WithYouWithMe's Veteran Pathway actively transition ex-service members into cyber roles, leveraging their disciplined problem-solving and threat-response abilities.[21]

ACS members have seen individuals from diverse professions, including lawyers, chefs, nurses, and accountants, excel in cyber security. These backgrounds provide highly valued strengths such as time management, multi-tasking, communication skills, and meticulous attention to detail. Employers consistently highlight these as core attributes in the cyber workforce.

No single industry is the dominant feeder for cyber talent. Instead, the transferable strengths found across the economy are what matter most, particularly when complemented with targeted technical training.

To harness the potential of transferrable skills, government should:

- Promote the use of the interoperable skills frameworks like SFIA – including through the National Skills Taxonomy – to create a shared language for recognising transferable skills
- Expand and streamline RPL so that professionals with relevant experience or certifications can transition into cyber roles more quickly
- Support micro-credentials and vendor certifications as stackable pathways that bridge non-technical experience with technical capability
- Provide employer incentives to take on career changers, recognising that non-traditional entrants often need initial support and mentoring to succeed.

References

[1] Australian Computer Society, Deloitte Access Economics. 2025. 'ACS Australia's Digital Pulse 2025'. https://www.acs.org.au/campaign/digital-pulse.html
[2] Australian Computer Society. 2025. 'Cyber Security Committee Members'. https://www.acs.org.au/governance/cybersecurity-committee/cybersecurity-committee-extended.html
[3] Seoul Accord. 2025. 'Accredited Programs'. https://www.seoulaccord.org/signatories.php?id=135
[4] Migration (LIN 19/051: Specification of Occupations and Relevant Assessing Authorities) Instrument 2019 https://www.legislation.gov.au/F2019L00278/latest/text
[5] Australian Computer Society. 2025. 'Cyber Security Occupations and ANZSCO codes'. https://www.acs.org.au/msa/information-for-applicants/occupations-anzsco-codes/cyber-security-occupations.html
[6] Digital Pulse 2025
[7] ibid
[8] Australian Public Service Commission. 10 March 2023. 'APS Digital Traineeship Program'. https://www.apsc.gov.au/initiatives-and-programs/aps-professional-streams/aps-human-resources-hr-profession/aps-hr-professional-news/aps-digital-traineeship-program
[9] Hays. 2025. 'The Hays 2025 Skills Report: Prepare for the Changing Face of Skills'. https://www.hays.com.au/documents/276732/1102429/PREPARE+FOR+THE+CHANGING+FACE+OF+SKILLS+-+The+Hays+2025+Skills+Report.pdf
[10] Insight Economics. 17 October 2024. 'Improving evaluation of economic impact in ICT procurement'. https://www.technology1.com/__data/assets/pdf_file/0007/267658/TechOne_Improving-economic-impact-evaluation-in-ICT-procurement_Final-Report_18-October-2024_Final.pdf
[11] https://www.industry.gov.au/publications/broader-economic-benefits-ict-sector-procurement
[12] Neagle, Rohan. January 16 2023. 'Hey, cyber security industry, do you want me or not?'. *Information Age*. https://ia.acs.org.au/article/2023/hey--cyber-security-industry--do-you-want-me-or-not--.html
[13] Rathbone, Jane. September 3 2024. 'Why can't I get a graduate job in cyber security?'. *Information Age*. https://ia.acs.org.au/article/2024/why-can-t-i-get-a-graduate-job-in-cyber-security-.html
[14] NCVER. 24 October 2024. 'VET qualification completion rates 2023.' https://www.ncver.edu.au/research-and-statistics/publications/all-publications/vet-qualification-completion-rates-2023
[15] NIST. November 18 2024. 'Unlocking Cybersecurity Talent: The Power of Apprenticeships'. https://www.nist.gov/blogs/cybersecurity-insights/unlocking-cybersecurity-talent-power-apprenticeships
[16] OECD. 2023. 'Building a Skilled Cyber Security Workforce in Five Countries'. https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/03/building-a-skilled-cyber-security-workforce-in-five-countries_82677fa2/5fd44e6c-en.pdf
[17] University of South Australia. 'Software Engineering Degree Apprenticeship' https://study.unisa.edu.au/short-courses/software-engineering-partner-program/
[18] Australian Computer Society. 'Vendor Certifications'. https://www.acs.org.au/msa/infohub/vendor-certifications.html
[19] MEGT, Deloitte Access Economics. 2025. 'MEGT's Productivity Prospectus: Unlocking productivity and prosperity through Australia's Apprenticeship system' https://www.megt.com.au/sites/default/files/documents/2025-08/MEGT%20Productivity%20Prospectus_FINAL.pdf
[20] Australian Computer Society. 2025. 'ACS Professional Year in IT' https://www.acs.org.au/cpd-education/professional-year-program.html
[21] https://withyouwithme.com/jobseekers/veteran-program/