

## AISA Calls for Diversity to Protect the Nation

27 May 2026:

Australia's peak cyber security body is calling for urgent national action to diversify the cyber workforce, warning the country cannot afford to leave critical talent untapped as cyber threats escalate and workforce shortages deepen.

The Australian Information Security Association (AISA) said Australia faces a growing cyber capability gap at the same time governments, critical infrastructure operators and businesses are confronting increasingly sophisticated threats.

Jobs and Skills Australia data showed around 70,900 Australians were employed as Database and Systems Administrators and ICT Security Specialists in August 2025, with employment in the sector projected to grow by 14.2 per cent by 2029, more than double the national average.

At the same time, more than 50 per cent of Australian Government agencies are already experiencing critical cyber security skills shortages, according to the State of the Service Report.

AISA Board Member and cyber expert Scarlett McDermott said Australia would struggle to meet future cyber capability demands unless governments and industry took stronger action to diversify by attracting more women, people who identify as women, First Nations people and people from disadvantaged backgrounds into the sector.

"Cyber security is now fundamental to Australia's national resilience, economic stability and public safety, but we are still drawing from a workforce pool that is far too narrow," Ms McDermott said.

"We cannot continue talking about cyber shortages while overlooking enormous talent pools across the Australian community."

"Women, for example, currently make up just 17 per cent of Australia's cyber security workforce. That figure alone shows we are nowhere near where we need to be."

AISA said improving diversity was not simply an equity issue, but a national capability issue. Research and workforce data by Industry Skills Australia continues to show that less diverse industries experience deeper and more persistent workforce shortages, while broader participation improves innovation, productivity and resilience.

Ms McDermott said cyber teams benefit from different lived experiences, cultural perspectives and problem-solving approaches, particularly as cyber threats increasingly target diverse communities, essential services and vulnerable Australians.

“Cyber attackers do not all think the same way, and our defenders cannot all come from the same backgrounds either,” she said.

“We need stronger pathways for women and people who identify as women, First Nations Australians, regional Australians, career changers and people from disadvantaged communities.”

“That means scholarships, paid pathways, mentoring, flexible work arrangements, targeted cadetships and far greater investment in cyber education and training.”

AISA is calling on governments to expand incentives and workforce initiatives that specifically support underrepresented groups entering cyber careers, including through schools, vocational education, universities and mid-career transition programs.

Ends

Chris Wagner 0434 378 939