# WOMEN IN CYBER SECURITY Summit

FEBRUARY 2025

GREAT HALL
PARLIAMENT HOUSE

CANBERRA


EVENT PARTNER

AISA Australian Information Security Association

EVENT PARTNER

HEMISPHERE EAST

MAJOR SPONSOR

infoblox

# Executive Summary

The Women in Cyber Summit, held at Parliament House in February 2025, brought together key figures from government, industry, education, and advocacy sectors to tackle the urgent need for greater diversity and inclusion in Australia's cyber security workforce.

With women currently making up only 17% of the national cyber workforce, the event highlighted the deep-seated barriers, the potential opportunities for change, and the crucial importance of diversity as a fundamental security requirement.

Discussions covered the economic and social impacts of cyber crime, the necessity of flexible career paths, and the vital roles of government, industry, and education in building a more inclusive workforce.

The consistent theme was that diversity is critical for national security, innovation, and productivity.

The summit featured insightful keynote addresses, engaging panel discussions, and practical strategies for how Australia can meet the growing demand for cyber security talent while simultaneously creating a fairer and more resilient workforce.

The Women in Cyber Security Summit 2025 was presented by AISA and Hemisphere East supported by major sponsor Infoblox.

# Event Overview

The summit was organised into six panel sessions, each exploring different aspects of diversity and inclusion within the cyber security workforce.

It showcased prominent speakers and panelists from government, industry, and advocacy, who shared their perspectives on overcoming obstacles, fostering collaboration, and creating practical pathways for underrepresented groups.

*"You can't be what you can't see. Be the role models of tomorrow."*
*Jacqui Loustau, Founder & Executive Director, AWSN*

# Opening Keynote


## Keynote by Dr Andrew Charlton, Special Envoy for Cyber Security & Digital Resilience

Dr. Andrew Charlton MP, the government's Special Envoy for Cyber Security and Digital Resilience, kicked off the summit with a keynote address.

He outlined the Australian government's view on the escalating cyber threat landscape and the pressing need for diversity in the sector. He highlighted the significant economic and social costs of cyber crime, which is projected to reach $10.5 trillion globally this year, and noted that Australia experiences a cyber attack every six minutes.

Dr. Charlton framed diversity as a security imperative, stressing that cyber security teams are stronger, more resilient, and better equipped to solve complex problems when they include individuals with diverse genders, backgrounds, and experiences.

Importantly, Dr. Charlton also relayed his own personal experience as a victim of cyber crime from his days prior to serving in government. This personal reflection proved to be extremely valuable as it showed that no-one is immune to the effects of cyber criminals.

He also pointed to specific government initiatives designed to address these barriers, such as micro-credentialing, flexible work models, and the professionalisation of the field, all aimed at increasing the participation of women and other underrepresented groups.

# Panel Session One

## Navigating the Cyber Frontier: The Current Landscape for Women

Panellists:

- Meg Tapia - Managing Director, Novexus
- Hamish Hansford - Deputy Secretary, Cyber, Digital and Technology Policy Division, Department of Home Affairs
- Jen Stockwell - National Security & Geopolitical Risk Principal, Telstra
- Jacqui Laustau - Managing Director, AWSN

## Overview

This panel delved into the systemic barriers women face in cyber security and the significant role diversity plays in driving innovation and national security.

Panelists shared personal stories of navigating challenging workplace cultures, pay disparities, and the undervaluing of non-traditional career paths. They stressed that diversity programs aren't just about fairness; they are essential for ensuring a true merit-based system, as women and underrepresented groups often lack the opportunities to showcase their skills.

Jen Stockwell emphasised the importance of diversity programs in creating equitable workplaces, while Jacqui Loustau highlighted the shared responsibility of all stakeholders to build talent pipelines that allow everyone to contribute to the cyber security workforce.

Panelists also discussed the vital role of mentorship and visible role models in overcoming systemic challenges.

## Key Points

- Systemic barriers like pay gaps and toxic cultures must be addressed.
- Diversity programs are vital for fostering meritocracy and innovation
- Mentorship and role models are crucial for creating lasting change.

# Panel Session Two

## From Awareness to Action: Pathways for Women in Cyber Security


Panellists:

- Annie Haggar - Partner, Head of Cyber Security, Norton Rose Fulbright
- Tupou Baravilala - Director General, Digital Government Transformation, Cyber Security, Ministry of the Republic of Fiji
- Phil Jenkinson - Chief Executive Officer, Baidam
- Kersti Eesmaa - Ambassador for Women in Cyber Security, WorkPath Australia
- Robert Le Busque - Regional Vice President and Managing Director Australia, NZ and India, Verizon

## Overview

This session focused on practical steps to create accessible and flexible pathways into cyber security for women and other underrepresented groups. Many panelists shared that their entry into the field was accidental, underscoring the need for more intentional and visible career routes.

Early intervention, starting at the primary school level, was highlighted as critical for building a diverse talent pipeline. Pip Jenkinson argued that expecting individuals from remote or regional communities to relocate for cyber security jobs is impractical and exclusionary.

Former Estonian Ambassador to Australia Kersti Eesmaa encouraged women to embrace their unique perspectives, noting that diversity isn't about becoming "as good as men" but about bringing complementary skills and perspectives to the table. The session also explored the effectiveness of scholarships, peer mentoring, and culturally relevant programs in fostering inclusion.

## Key Points

- Intentional and accessible pathways are essential for workforce diversity
- Early intervention and culturally relevant education programs are critical
- Flexible work arrangements are key to inclusion, especially for regional and remote communities

# Keynote Panel

## Empowering Women in Cyber Security: Australia’s next line of digital defenders

Panellists:

- Lieutenant General Michelle McGinness CSC - National Cyber Security Coordinator
- Brendan Dowling - Ambassador for Cyber Affairs and Critical Technology
- Amy Farrow - Chief Information Officer, Infoblox

## Overview

A major highlight of the summit was a keynote panel featuring Lieutenant General Michelle McGuinness, National Cyber Security Coordinator; Amy Farrow, Global CIO of Infoblox; and Brendan Dowling, Ambassador for Cyber Affairs and Critical Technology. This discussion connected diversity to national security, economic prosperity, and innovation.

Lieutenant General McGuinness stressed that diversity is not just a capability—it is a fundamental necessity for Australia’s security and sustainability. Amy Farrow shared her personal journey of overcoming gender barriers and highlighted the immense value of diverse thinking in tackling cyber security challenges.

Ambassador Dowling framed cyber security as more than a technical issue, positioning it as a gender equality and development challenge that requires inclusive capacity building. The panelists also addressed practical strategies for increasing representation, including the importance of gaming as an entry point for young women and the role of mentorship in breaking down barriers.

## Key Points

- Diversity is essential for national security and economic productivity
- Cyber security must be reframed as a broad societal issue, extending beyond just technology
- Mentorship and visible leadership are critical for empowering women in the field

# Panel Session Three

## Equity and the Opening of Alternate Pathways for Talent: Training and Education in Cyber Security

Panellists:

- Alison Wall - Deputy Chief Executive Officer, Future Skills Organisation
- Scarlett McDermott - Board Director, AISA
- Julia Burns - Chair TAFECyber
- Jacqui Loustau, Managing Director, AWSN
- Matt Sailer - Chief Executive Officer, Australian Cyber Collaboration Centre

## Overview

This session examined alternative routes into cyber security and the importance of recognising diverse skills and backgrounds. Panelists emphasised the need to broaden the perception of what constitutes cyber security expertise, valuing cognitive diversity, business acumen, and transferable skills alongside technical expertise.

Panelists highlighted the challenges posed by inflexible training programs, cultural barriers in workplaces, and the lack of visible role models. Solutions discussed included rebranding cyber security to emphasise its societal impact, job-sharing initiatives, and embedding cyber security awareness across all industries.

The value of mentorship, sponsorship, and allyship was repeatedly emphasised as key to attracting and retaining diverse talent.

## Key Points

- Broader recognition of diverse skills is essential in cyber security.
- Flexible and inclusive training programs can break down barriers.
- Mentorship and allyship are critical for fostering an inclusive workforce.

# Panel Session Four

## Strengthening the Cyber Pipeline: Government and Industry Working Together

Panellists:

- Peter Anstee - First Assistant Secretary, Cyber and Technology Security Policy, Department of Home Affairs
- Keryn McMartin - Identity Consultant, IdentityXP
- Craig Ford - Board Director, AISA
- Jacqui Kernot - Vice President, Thales Cyber Solutions ANZ and CEO, Tesserent
- Jakub Zverina - Program Manager, Organisation Capability, CyberCX

## Overview

This session focused on collaboration between government, industry, academia, and advocacy to build a robust and diverse cyber security workforce. Panelists discussed the persistent disconnect between education and employment opportunities, as well as the lack of flexible training options and regional access.

Jakub Zverina from CyberCX highlighted the importance of partnerships in leveraging collective expertise and resources, while Craig Ford from AISA called for more action-oriented solutions, such as traineeships and job placements.

The session also addressed the need for accountability through diversity targets and procurement policies to drive cultural change in the sector.

## Key Points

- Collaboration across sectors is essential for building a resilient workforce
- Accountability measures, such as diversity targets, can drive cultural change
- Practical solutions like traineeships and job placements are needed to address workforce shortages


# Panel Session Five

## The Next Chapter: Women In Cyber Security Paving the Way Forward

Panellists:

- Laura O’Neill - Head of Advisory & Assurance, Fujitsu Australia
- Jacqui Nelson - Chief Executive Officer, Dekko Secure
- Emma Jones - Founder, Project F
- Lieutenant General Susan Coyle AM CSC DSM - Chief Joint Capabilities, Department of Defence

## Overview

Our final panel brought together leaders from defence, industry, startups, and advocacy to discuss the next chapter for women in cyber security. The discussion covered personal career journeys, strategies for building diverse and inclusive teams, the importance of mentorship and sponsorship, and practical steps organisations can take to improve gender diversity and inclusion in the sector.

Panelists shared their experiences and insights on advancing women in cyber security, emphasising that real change requires intentional action by leaders at all levels.

Key topics included removing barriers in hiring, fostering inclusive cultures, the critical role of advocacy and sponsorship, and the need for intersectional approaches to diversity.

The panel also highlighted the importance of early engagement with students, collaboration between industry and academia, and the necessity of benchmarking organisational practices against national standards.

## Key Points

- Leadership must drive intentional, everyday actions to create inclusive and empowering workplaces for all
- Removing barriers and fostering mentorship, sponsorship, and flexible work are essential to advancing diversity in cyber security
- Accountability and collaboration—across organisations, academia, and industry—are crucial for sustainable progress in gender and diversity inclusion



# Observations

The seven unique sessions held during the day were engaging, vibrant, and sparked lively conversations, as shown by the fact that each Q&A session ended with many audience members still eager to ask their questions.

Some of the most insightful questions and observations came from a group of Year 12 students from Macarthur Anglican School, and it was apparent that for the 2026 Women in Cyber Summit, a considerable focus should be on gathering more school age students as panellists and delegates.

# Key Recommendations

one

## Set Diversity Targets

Establish clear benchmarks for diversity and inclusion across government agencies and contractors in cyber security.

two

## Flexible and Accessible Pathways

Set Diversity Targets: Establish clear benchmarks for diversity and inclusion across government agencies and contractors in cyber security.

three

## Early Education

Embed cyber security awareness and skills into primary and secondary school curricula.

four

## National Mentorship Programs

Create a national mentorship initiative to support women and minorities entering and advancing in cyber security.

# Key Recommendations

five

## Collaboration Workforce Programs

Facilitate partnerships between government, industry, and academia to co-design inclusive career pathways.

six

## Accountability Mechanisms

Use procurement policies to incentivise diversity and inclusion in cyber security contracts.

seven

## Promote Role Models

Highlight diverse leaders in cyber security through public campaigns to inspire the next generation.

eight

## Support 2026 Summit

We seek the support of the Department of Home Affairs and Department of Education in delivering the 2026 Summit to ensure the goals of the government are woven into next year's event for maximum impact to the Australian community.