Working with Women Alliance

Australian Multicultural Women's Alliance

Department of Home Affairs

Via Email: CSSH2@homeaffairs.gov.au

Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Dear Department of Home Affairs,

The Working with Women Alliance (WwWA) and the Australian Multicultural Women's Alliance (AMWA) welcomes the opportunity to consult on *Horizon 2 of the 2023-2030 Australian Cyber Security Strategy*. The insights provided pertain to questions six and 14 of the Discussion Paper and highlight the ways in which women face disproportionate risks and impacts from cyber incidents.

Women are more likely to engage with social and health services for themselves and their children[1] and are also overrepresented as recipients of income support payments.[2] This necessitates a broad digital footprint which places them at heightened risk when cyber-attacks occur, as their personal and sensitive information is stored across multiple systems. Further, gender stereotypes and cultural biases contribute to women's overexposure to abuse via technology.

Financial Abuse

Women are more likely than men to be victims of financial abuse, including through cyber incidents such as identity theft and coerced account access.[3] Women are also statistically more likely to experience bank card fraud.[4] The direct impact of such abuse is

[1] *Patient Experiences 2023-24 Financial Year.* (2024). Australian Bureau of Statistics. https://www.abs.gov.au/statistics/health/health-services/patient-experiences/latest-release#data; Australian Institute of Health and Welfare, 2025, *Specialist homelessness services annual report 2023–24*, https://www.aihw.gov.au/reports/homelessness-services/specialist-homelessness-services-annual-report/contents/clients-services-and-outcomes

[2] *Expanded DSS Benefit and Payment Recipient Demographics - June 2025,* 2025, data.gov.au, https://data.gov.au/data/dataset/dss-payment-demographic-data

[3] Commonwealth Bank of Australia & Deloitte Access Economics, 2022, *The cost of financial abuse in Australia,* https://www.commbank.com.au/content/dam/caas/newsroom/docs/Cost%20of%20financial%20abuse%20in%20Australia.pdf

[4] ABS, 2025, *Personal Fraud*, https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release#card-fraud

considerable, with costs to victims estimated at $5.7 billion.[5] For migrant and refugee women, identity theft risks are compounded by low systems literacy, language barriers, and potential mistrust of authorities, which limit access to redress and support.

Migrant and Refugee Communities

Online scams directed at migrant and refugee communities are particularly aggressive and successful. Members of such communities report higher average financial losses through scams[6] and women are less likely to report identity theft due to mistrust of authorities, fear of shaming or ostracism within their communities, and concerns about confidentiality. Women on partner or temporary visas may be manipulated via threats to their immigration status, including deportation or visa invalidation, with perpetrators targeting their reliance on, and exclusion from, critical systems.

Online and Technology-Facilitated Abuse

Women are significantly more likely than men to experience sexual and gendered abuse online.[7] Such abuse tends to be more severe and psychologically damaging.[8] Risks are further elevated for women experiencing multiple forms of discrimination, including First Nations women, migrant and refugee women, women with disability, and LGBTIQ+SB communities. There are substantial gendered components to technology-facilitated abuse, with women more likely to experience incidents like stalking, surveillance, and receiving abusive online messages, often from male perpetrators and intimate partners.[9]

Deepfakes

Deepfake pornography has emerged as a particularly harmful form of technological abuse that disproportionately impacts women. A 2023 study found that 98% of deepfake content

---

[5] ibid.
[6] Australian Competition & Consumer Commission, 2022, *Scam losses to culturally diverse communities, people with disability and Indigenous Australians almost doubled in 2021,* https://www.accc.gov.au/media-release/scam-losses-to-culturally-diverse-communities-people-with-disability-and-indigenous-australians-almost-doubled-in-2021
[7] eSafety Commissioner, 2025, Online risks for women, https://www.esafety.gov.au/women/online-risks-for-women
[8] ibid.
[9] Anatasia Powell, Asher Flynn, Sophie Hindes, 2022, *Technology-facilitated abuse: National survey of Australian adults' experiences,* ANROWS, https://anrows-2019.s3.ap-southeast-2.amazonaws.com/wp-content/uploads/2022/07/27172214/4AP.3-Flynn-TFa3-Survey-of-VS.pdf

online was pornographic, and 99% of that content targeted women and girls.[10] These tools facilitate sexual bullying in ways that are rapidly outpacing regulatory or protective measures. Since deepfakes can be posted, reposted, resurfaced, or amplified online, their visibility and accessibility often result in ongoing and long-lasting effects.

Digital Literacy Programs

A strong example of an effective cyber awareness program is U Right Sis?,[11] a primary prevention initiative led by Aboriginal and Torres Strait Islander communities, in partnership with specialist domestic, family, and sexual violence (DFSV) services, to address technology-facilitated abuse (TFA) in remote Central Australia. By grounding its approach in Aboriginal knowledge and lived experience, U Right Sis? has developed locally relevant tools that both challenge harmful attitudes and support women and young people to stay safe online. Delivered in regions with high need and historically limited cyber-safety resources, U Right Sis? provides safe, trauma-informed spaces for participants to learn, share, and act. Over three years, the program has delivered 39 workshops and engaged with 251 participants,[12] many of which requested repeat delivery, reflecting a demand for ongoing engagement. Independent evaluation found that participants' understanding of TFA increased from 75% pre-workshop to 100% post-workshop and stakeholders reported stronger knowledge of reporting pathways and confidence in responding to TFA, while also observing shifts in community attitudes.[13] Further support should focus on scaling U Right Sis? through a train-the-trainer model, embedding the program within local organisations to ensure sustainability and equitable access.

The Digital Sisters program[14] by the Good Things Foundation Australia demonstrates the importance of grassroot involvement in the effectiveness of cyber awareness messaging. Delivered through local community organisations with bilingual digital mentors, the

---

[10] eSafety Commissioner, 2024, *Addressing deepfake image-based abuse*, https://www.esafety.gov.au/newsroom/blogs/addressing-deepfake-image-based-abuse

[11] U Right Sis?, https://www.urightsis.com/

[12] Brown, C., 2025, *The Evaluation of the 'U Right Sis? Staying Safe Online' Program: Final Report*, Her Story Mparntwe, https://static1.squarespace.com/static/66e0dbc8b41728163dda5ecf/t/68abfdd36fd813567df723ba/1756102099762/URS+Program+Evaluation+Full+Report_Digital+250825.pdf

[13] ibid.

[14] Good Things Foundation Australia, Digital Sisters, https://goodthingsaustralia.org/our-programs/digital-sisters/

program supports migrant and refugee women to stay safe online using easy English and culturally responsive approaches. Since its rollout in 2023, Digital Sisters has reached more than 4,500 women across 55 community organisations, with 88% of participants reporting improved digital skills.[15] Sustained and appropriately structured funding will be essential to maintain impact and ensure equity of access.

Through over 3,000 community partners, the Be Connected Network has helped more than two million older Australians[16] build digital literacy and online safety skills. A 2020 evaluation of the program demonstrated a social return on investment of $4.01 for every $1 invested.[17] We note its structure as a useful model of how community-led approaches are critical in empowering diverse populations to become more cyber aware.

It is essential that Australia's cybersecurity strategy and regulation recognise the gendered dimensions of cyber incidents, and in doing so, support investment in community-led, culturally credible programs that centre women and are accessible, trusted, and effective in preventing and responding to cyber harms. Women, particularly migrant and refugee women, face challenges that differ both in nature and severity from the general population, and these must be reflected in the 2023-2030 Australian Cyber Security Strategy.

We look forward to continued engagement with the Department of Home Affairs on the development of an inclusive and gender-responsive Australian Cyber Security Strategy.

Yours sincerely,

Dr Gemma Killen
Director – National Women's Equality
Working with Women Alliance

Malini Raj
Executive Director
Australian Multicultural Women's Alliance

[15] ibid.
[16] eSafety Commissioner, 2024, *2 million learners and counting: seniors choose to Be Connected online*, https://www.esafety.gov.au/newsroom/media-releases/2-million-learners-and-counting-seniors-choose-to-be-connected-online
[17] Department of Social Services, 2020, *Evaluation of Be Connected*, https://www.dss.gov.au/improving-digital-skills-older-australians/resource/evaluation-be-connected