



20 July 2026

**SUBMISSION TO THE DEPARTMENT OF SOCIAL SERVICES**  
**Feedback on the Second Action Plan of the National Plan To End Violence**  
**Against Women and Children 2022–2032**

**From: SOROPTIMIST INTERNATIONAL AUSTRALIA INC (SI AUSTRALIA)**  
**Club Lead: Soroptimist International of Brisbane Inc (SI Brisbane)**

**Safety, Sovereignty, and Sustainability: Protecting Women and**  
**Children From Emerging Technological Harm and Economic Precarity**

## **1.0 INTRODUCTION**

### **1.1 About Soroptimist International Australia**

Soroptimist International Australia Inc (SI Australia) represents 55 clubs nationally and operates within the Soroptimist International South East Asia and Pacific (SISEAP) Federation across 13 countries. As part of a global network of more than 66,000 members in 118 countries, Soroptimist International holds General Consultative Status with the United Nations Economic and Social Council (ECOSOC).

SI Australia advocates for the human rights, safety and empowerment of women and girls through evidence-based policy engagement and practical action. Our upstream advocacy framework translates international human rights standards and global commitments into structural domestic policy and legislative reform.

Our work contributes directly to:

- SDG 4: Quality Education
- SDG 5: Gender Equality, particularly Target 5.2 on eliminating violence against women and girls
- SDG 10: Reduced Inequalities
- SDG 11: Sustainable Cities and Communities
- SDG 16: Peace, Justice and Strong Institutions.

## 1.2 Purpose of this Submission

SI Australia welcomes the opportunity to contribute to the development of the **Second Action Plan** under the **National Plan to End Violence against Women and Children 2022–2032**.

We support the consultation paper's emphasis on evidence-informed action, whole-of-system responses and addressing emerging forms of violence that are reshaping how harm is experienced and perpetrated (Department of Social Services, 2026). Our submission focuses on the critical intersection between technology, structural economic inequality and domestic, family and sexual violence (DFSVM). We submit that technology-facilitated abuse (TFA), algorithmic profiling, housing insecurity, digital exclusion and punitive compliance systems represent significant and evolving risk factors requiring explicit attention.

Consistent with the National Plan's life-course approach, SI Australia advocates for structural interventions that place the safety, economic security, dignity and agency of victim-survivors at the centre of policy responses (Commonwealth of Australia, 2022; United Nations, 2015).

SI Australia encourages the Second Action Plan to adopt a future-ready approach that anticipates emerging forms of technology-facilitated abuse and addresses the structural conditions that may increase vulnerability to domestic, family and sexual violence in an increasingly digital society.

## 2.0 PRIORITY AREA 1: VICTIM-SURVIVORS

### 2.1 Technology-Facilitated Abuse and Coercive Control

Technology-facilitated abuse has emerged as an increasingly pervasive and sophisticated form of coercive control. Perpetrators increasingly exploit internet-connected devices, smart home technologies, social media platforms and location services to monitor movements, isolate victim-survivors and exert control (Australian National Research Organisation for Women's Safety [ANROWS], 2020; eSafety Commissioner, 2024a).

As outlined in our Digital Safety Futures Framework (Sorooptimist International Australia, 2026a), women experiencing TFA often incur substantial costs to restore digital safety, including replacing devices, securing networks, obtaining specialist technical assistance, and relocating communication services. These costs compound economic insecurity and can create additional barriers to leaving abusive relationships (ANROWS, 2020; eSafety Commissioner, 2024a).

The **Second Action Plan** must account for major advancements in Australia's regulatory landscape designed to curb these harms. Crucially, the enforcement of the Online Safety Amendment (Social Media Minimum Age) Act 2024 on 10 December 2025 mandates that age-restricted social media platforms take reasonable steps to prevent children under 16 from creating or maintaining accounts, backed by civil penalties of up to \$50 million for corporate non-compliance (eSafety Commissioner, 2025; UNICEF Australia, 2024).

This structural age-gate works alongside the Privacy and Other Legislation Amendment Act 2024, which achieved Royal Assent on 10 December 2024 and enacted a first tranche of critical privacy protections (Parliament of Australia, 2024; Sparke Helmore Lawyers, 2025). This landmark legislation introduced targeted

criminal offences to respond to doxxing (the malicious exposure of personal information online) and established a new statutory tort for serious invasions of privacy—actionable without proof of damage—which officially commenced on 10 June 2025 (Astris Law, 2026; Parliament of Australia, 2024; Sparke Helmore Lawyers, 2025).

Soroptimist International Australia strongly urges the Department of Social Services to explicitly account for the escalation of automated, generative, and agentic artificial intelligence (AI) systems within the Second Action Plan. Recent 2026 foundational research, *Artificial Intelligence, Coercive Control, and Foreseeable Risk in Domestic and Family Violence Contexts*, directly underscores that advanced AI tools have fundamentally shifted the landscape of technology-facilitated abuse. Perpetrators are increasingly leveraging these technologies to automate complex multi-platform surveillance, generate highly realistic and weaponised non-consensual deepfakes, and significantly lower the technical barriers to executing psychological, economic, and reputational harm.

Critically, this research exposes a severe ‘institutional lag,’ demonstrating that our judicial systems and law enforcement frameworks remain structured around reactive, physical definitions of harm, routinely failing to disrupt cumulative and automated digital violence. We contend that the Commonwealth must reject the policy trap of ‘waiting for deep quantitative data trails’ before introducing strict regulatory constraints on automated public and private sector systems. Because the mechanisms of generative AI abuse mirror and amplify known patterns of coercive control, this systemic harm is legally foreseeable.

The Second Action Plan must adopt a proactive, safety-by-design framework that mandates human-safety triggers and automated risk assessments across all digital and public infrastructure, treating technological safety not as an afterthought, but as a core pillar of women’s structural and economic security.

The Second Action Plan should explicitly integrate these statutory mechanisms, recognising TFA as a distinct and evolving manifestation of domestic, family and sexual violence requiring nationally consistent legislative and service responses that leverage these new legal rights and protections.

#### **ILLUSTRATIVE CASE EXAMPLE 1: Technology-Facilitated Abuse and Smart Home Surveillance**

*Cross-reference: Section 2.1 and Recommendation 3*

**Scenario:** A woman separates from an abusive partner and relocates with her children. Despite physical separation, the perpetrator retains remote access to internet-connected devices previously installed in the family home, including smart cameras, location-sharing applications and environmental home systems. Through these technologies, he monitors her movements, tracks communications and exerts coercive control. To restore her safety, she incurs substantial costs replacing devices, changing accounts and obtaining specialist technical assistance.

**System issue:** Technology-facilitated abuse extends beyond online harassment and can weaponise consumer technologies long after physical separation. The practical and financial burden of remediating digital abuse frequently falls upon victim-survivors.

**Policy implication:** The Second Action Plan should recognise digital surveillance as a mechanism of coercive control and strengthen Safety by Design approaches across consumer technologies (ANROWS, 2020; eSafety Commissioner, 2024a; Soroptimist International Australia, 2026a).

## 2.2 Housing Security and Structural Barriers

Safe and affordable housing remains one of the most significant determinants of whether women and children can safely leave violent relationships (Australian Institute of Health and Welfare, 2025; Everybody's Home, 2025).

As explored in our Submission to the Senate Inquiry into Intergenerational Housing Inequity (Sorooptimist International Australia, 2026b), increasing reliance on automated tenancy screening and data-driven rental assessments may inadvertently disadvantage victim-survivors whose housing histories reflect emergency relocations, rent arrears arising from financial abuse or broken leases associated with safety concerns.

Digital records held in third-party rental databases can create persistent barriers to securing future accommodation, increasing the risk of housing insecurity and homelessness among women and children (Australian Housing and Urban Research Institute, 2024; Everybody's Home, 2025).

### ILLUSTRATIVE CASE EXAMPLE 2: Housing Insecurity and Automated Decision-Making

*Cross-reference: Section 2.2 and Recommendation 4*

**Scenario:** A woman leaves a violent relationship and enters emergency accommodation with her children. Due to acute financial abuse and urgent relocation, she accumulates rent arrears and terminates her lease early. When applying for private rental accommodation, she is repeatedly rejected by automated screening platforms without being given a human point of contact or visibility over how her data has been assessed.

**System issue:** Automated decision-making platforms may reproduce and entrench historical disadvantage by treating safety-driven housing disruptions as indicators of financial risk.

**Policy implication:** The Second Action Plan should establish safeguards and human review mechanisms to prevent automated tenancy platforms from discriminating against victim-survivors of domestic and family violence (Australian Housing and Urban Research Institute, 2024; Everybody's Home, 2025; Sorooptimist International Australia, 2026b).

## 2.3 The Intersecting Impact of Punitive Welfare Compliance

Economic dependency is frequently used as a mechanism of coercive control. For victim-survivors attempting to establish independence, interactions with mainstream employment systems can sometimes compound, rather than alleviate, existing vulnerabilities.

As established in *Shaping an Equitable Future: A Gender-Responsive Blueprint for Australian Employment Services* (Sorooptimist International of Brisbane, 2026b), automated compliance mechanisms may disproportionately affect single parents and women navigating crisis recovery by imposing rigid requirements that fail to account for circumstances such as domestic violence, housing instability and digital exclusion.

These impacts may be further compounded for culturally and linguistically diverse women, First Nations women and women with disabilities. When employment systems do not adequately account for crisis circumstances, they risk undermining the financial independence that is often essential to escaping coercive control.

## **2.4 App-Based Financial Sabotage and Corporate Accountability**

SI Australia strongly advocates for the Second Action Plan to establish mandatory, enforceable economic safety triggers across the digital banking and financial services sector. Data released by the NSW Bureau of Crime Statistics and Research (BOCSAR) and Legal Aid NSW reveals a profound overlap between digital tools and economic coercion, with 60% of recorded coercive control incidents involving direct digital harassment, monitoring, and tracking.

A critical vector of this harm is tech-facilitated financial sabotage. Perpetrators are weaponising routine consumer interfaces—maliciously tracking victim-survivors through banking apps, toll accounts, and shared utility portals, while intentionally accumulating debilitating debts under a partner’s name. Furthermore, the exploitation of micro-transaction description fields (often transfers of less than \$1 accompanied by abusive or threatening text) remains an insidious, hard-to-block channel for ongoing harassment and stalking.

While voluntary updates to the Australian Banking Association (ABA) Industry Guidelines and select banking terms are positive steps, a self-regulatory approach is entirely insufficient to protect women's economic security. Because banks are statistically among the very first institutions to detect an abusive relationship—often before specialist domestic violence services are engaged—the Commonwealth must legislate proactive ‘Safety by Design’ mandates.

The Second Action Plan must require financial institutions to implement real-time, automated disruption protocols. These must include immediate AI-driven filtering of abusive transaction text, strict limitations on cross-account digital tracking, and automated ‘financial safety flags’ that freeze suspicious debt accumulation and trigger trauma-informed support pathways. True upstream advocacy means shifting the burden of protection off the victim-survivor and onto the digital infrastructure that permits the abuse.

## **3.0 PRIORITY AREA 2: PREVENTION AND EARLY INTERVENTION**

### **3.1 Safety by Design and Digital Prevention**

Prevention efforts must keep pace with rapidly evolving technologies. The Safety by Design approach provides an important framework for reducing opportunities for technology-enabled abuse before harms occur (eSafety Commissioner, 2024a).

Digital platforms connected consumer technologies, and generative artificial intelligence tools should incorporate safeguards within their core architecture rather than relying on individual victim-survivors to navigate complex protective measures after abuse has occurred.

### **3.2 Digital Literacy and Community Capability**

Primary prevention requires sustained investment in community-led digital literacy and capability initiatives. Building localised capability enables women to identify indicators of technology-enabled abuse, secure their communications and safely access support services. These initiatives should be trauma-informed, culturally responsive and delivered in accessible formats to reduce systemic isolation and improve safety outcomes (Australian Digital Inclusion Alliance, 2025; eSafety Commissioner, 2025).

## 4.0 PRIORITY AREA 3: CHILDREN AND YOUNG PEOPLE IN THEIR OWN RIGHT

Children and young people are increasingly exposed to sophisticated forms of online harm, including image-based abuse, online misogyny and AI-generated sexual exploitation material (ANROWS, 2024; eSafety Commissioner, 2024b).

The rapid deployment of generative artificial intelligence technologies has increased both the scale and accessibility of these harms, resulting in significant psychological distress, reputational harm and social isolation among young people (ANROWS, 2024; eSafety Commissioner, 2025). Children and young people should be recognised as victim-survivors in their own right, with policy settings proactively adapted to protect their digital environments and developmental wellbeing.

### ILLUSTRATIVE CASE EXAMPLE 3: Children and AI-Generated Image Abuse

*Cross-reference: Section 4.0 and Recommendation 6*

**Scenario:** A secondary school student becomes the target of explicit synthetic sexual images generated using freely available consumer artificial intelligence applications and circulated online. Despite no intimate images existing, the student experiences intense humiliation, trauma and social isolation, leading to withdrawal from school activities.

**System issue:** Generative AI tools are creating new forms of image-based abuse and peer-to-peer exploitation that existing prevention and legal frameworks are struggling to address.

**Policy implication:** The Second Action Plan should incorporate early intervention frameworks addressing AI-enabled harms, online misogyny and synthetic image abuse targeting minors (ANROWS, 2024; eSafety Commissioner, 2024b, 2025).

## 5.0 PRIORITY AREA 4: PEOPLE WHO USE VIOLENCE

Technology has significantly expanded the means through which violence can be perpetrated. Digital systems allow perpetrators to monitor communications, track locations, control finances, and impersonate victim-survivors remotely (ANROWS, 2020; eSafety Commissioner, 2024a).

The Second Action Plan should modernise perpetrator intervention frameworks by incorporating digital abuse indicators into formal risk assessment tools. Case managers, law enforcement officers and perpetrator intervention programs require the capability to identify and respond to technology-facilitated coercive control at an early stage, thereby shifting responsibility for behavioural change away from victim-survivors.

## 6.0 PRIORITY AREA 5: SYSTEM INTEGRATION AND WORKFORCE

### 6.1 Digital Inclusion and Regional Safety

Access to reliable telecommunications infrastructure is increasingly essential for safety, help-seeking and recovery. For many women and children in regional, rural and remote communities, physical safety is intricately linked to digital inclusion and connectivity (Australian Digital Inclusion Alliance, 2025).

As documented in SI Brisbane's Submission to the Parliamentary Inquiry into Access to and Affordability of Medical Specialists in Australia (Soroptimist International of Brisbane, 2026a), healthcare and specialist service shortages in regional communities are often compounded by telecommunications limitations. When connectivity is unreliable or unaffordable, telehealth services, online counselling, emergency safety planning and timely access to crisis services can become significantly constrained.

#### **ILLUSTRATIVE CASE EXAMPLE 4: Regional Digital Exclusion and Access to Safety**

*Cross-reference: Section 6.1 and Recommendation 5*

**Scenario:** A woman living in a remote regional community experiences escalating domestic violence and attempts to implement a safety plan. Unreliable mobile infrastructure and cost-prohibitive internet connectivity prevent her from accessing online crisis counselling, obtaining legal information and maintaining a secure digital record of abuse. The nearest specialist service is several hours away.

**System issue:** Telecommunications black spots and digital exclusion can significantly impede a victim-survivor's capacity to seek help and access support.

**Policy implication:** The Second Action Plan should recognise telecommunications and digital connectivity as essential safety infrastructure (Australian Digital Inclusion Alliance, 2025; Soroptimist International of Brisbane, 2026a).

### **6.2 Workforce Capability and Cross-System Responses**

Effective responses to technology-facilitated abuse require workforce capability across law enforcement, education, healthcare, housing and community services.

Frontline workers require a greater understanding of the intersection between physical violence and digital control (ANROWS, 2020; eSafety Commissioner, 2024a). Cross-sector information-sharing arrangements should be governed by robust trauma-informed protocols that protect victim-survivor safety and privacy.

### **6.3 Emerging Risks and Future Readiness**

The accelerating pace of technological innovation is fundamentally reshaping the landscape of domestic, family and sexual violence. As highlighted in our Submission to the Inquiry into Artificial Intelligence and Data Centres (Soroptimist International Australia, 2026c), increasingly sophisticated computational systems and algorithmic decision-making models have emerged more rapidly than the policy frameworks needed to assess their implications for safety and equity.

When digital platforms and automated systems are used to inform decisions relating to housing, employment services and financial access, they may inadvertently reinforce structural disadvantage experienced by victim-survivors (Soroptimist International Australia, 2026b, 2026c).

Future readiness requires governments to move beyond reactive policy responses and establish ongoing horizon-scanning mechanisms capable of identifying and mitigating emerging technological risks before harms become widespread (Department of Social Services, 2026; United Nations, 2015).

### ILLUSTRATIVE CASE EXAMPLE 5: Emerging Technologies and Future System Risks

Cross-reference: Sections 6.3 and Recommendations 1, 4 and 7

**Scenario:** A woman escaping coercive control interacts with multiple essential digital systems to rebuild her life, including automated rental screening platforms, employment services compliance systems, online financial platforms and digital identity verification processes. Historical data disruptions caused by abuse trigger automated risk indicators across interconnected systems, leading to repeated barriers without meaningful human review.

**System issue:** Without trauma-informed safeguards, automated systems may transform historical disadvantage into ongoing barriers to recovery.

**Policy implication:** The Second Action Plan should collaborate with regulatory bodies to develop trauma-informed safeguards governing algorithmic decision-making across essential social and economic systems (Soroptimist International Australia, 2026b, 2026c; Department of Social Services, 2026).

## 7.0 CONCLUSION

The evidence presented in this submission demonstrates that technology, digital infrastructure and automated decision-making systems are increasingly shaping both the risk environment and recovery pathways for victim-survivors of domestic, family and sexual violence.

A future-ready Second Action Plan must therefore anticipate emerging harms and embed safety, equity and trauma-informed design across digital, social and economic systems (Commonwealth of Australia, 2022; Department of Social Services, 2026; United Nations, 2015).

## 8.0 SUMMARY RECOMMENDATIONS

SI Australia recommends that the Second Action Plan:

1. Recognise technology-facilitated abuse, AI-enabled coercive control and synthetic image exploitation as distinct forms of domestic, family and sexual violence requiring dedicated national action.
2. Embed Safety by Design principles and proactive financial safety triggers across consumer technologies, digital banking platforms, and generative AI systems to minimise opportunities for stalking, tracking, debt exploitation, and non-consensual image manipulation.
3. Establish nationally consistent protocols and specialised toolkits for identifying and responding to technology-facilitated abuse across justice, housing, health, employment and community services.
4. Develop safeguards ensuring that tenancy technologies, credit scoring systems and automated welfare decision-making processes do not disadvantage victim-survivors of domestic and family violence.

5. Recognise regional telecommunications and digital connectivity as essential safety infrastructure and support targeted digital inclusion, affordability and literacy initiatives for regional, rural and remote communities.
6. Expand age-appropriate prevention initiatives addressing online misogyny, digital consent, synthetic media abuse and technology-facilitated coercive control among children and young people.
7. Ensure employment and human service systems adopt trauma-informed approaches that appropriately respond to circumstances of domestic violence, housing instability and digital remediation.
8. Establish a permanent interdisciplinary national horizon-scanning mechanism involving specialist domestic and family violence services, technology experts, academia and victim-survivors to monitor and respond to emerging technology-facilitated harms.



**SI South East Asia Pacific 2026 - 2028**  
**EMPOWERING FUTURES**

## REFERENCES

Astris Law. (2026). *Australia's new statutory privacy tort (2025)*. <https://www.astrislaw.com.au>

Australian Bureau of Statistics. (2024). *Housing occupancy and costs*. <https://www.abs.gov.au>

Australian Digital Inclusion Alliance. (2025). *Australian Digital Inclusion Index 2025*.  
<https://www.digitalinclusionindex.org.au>

Australian Housing and Urban Research Institute. (2024). *An effective homelessness services system for older Australians* (AHURI Final Report No. 322). <https://www.ahuri.edu.au>

Australian Institute of Health and Welfare. (2025). *Specialist homelessness services annual report 2024–25*.  
<https://www.aihw.gov.au>

Australian National Research Organisation for Women's Safety. (2020). *Technology-facilitated abuse and domestic violence: Literature review*. <https://www.anrows.org.au>

Australian National Research Organisation for Women's Safety. (2024). *Young people, technology and domestic, family and sexual violence*. <https://www.anrows.org.au>

Commonwealth of Australia. (2022). *National Plan to End Violence against Women and Children 2022–2032*. Department of Social Services.

Department of Social Services. (2026). *Evidence to action: Informing direction for the Second Action Plan under the National Plan to End Violence against Women and Children 2022–2032*. Commonwealth of Australia.

eSafety Commissioner. (2024a). *Technology-facilitated abuse and coercive control*. <https://www.esafety.gov.au>

eSafety Commissioner. (2024b). *State of play: Youth, kids and digital dangers*. <https://www.esafety.gov.au>

eSafety Commissioner. (2025). *Social media age restrictions compliance report*. <https://www.esafety.gov.au>

Everybody's Home. (2025). *Women and housing insecurity in Australia*. <https://everybodyshome.com.au>

Harris, J., & Wood, M. (2026). *Artificial intelligence, coercive control, and foreseeable risk in domestic and family violence contexts*.

NSW Bureau of Crime Statistics and Research & Legal Aid NSW. (2025). *'It can hide in plain sight': The rise of technology-facilitated coercive control*.

Parliament of Australia. (2024). *Privacy and Other Legislation Amendment Bill 2024*. <https://www.aph.gov.au>

Soroptimist International. (2022). *Where we stand: Cyberbullying*. <https://www.soroptimistinternational.org>

Soroptimist International. (2023). *Where we stand: Violence against women and girls*. <https://www.soroptimistinternational.org>

Soroptimist International. (2024a). *Where we stand: Women and technology*. <https://www.soroptimistinternational.org>

Soroptimist International. (2024b). *Where we stand: Women in the urban environment*. <https://www.soroptimistinternational.org>

Soroptimist International. (2025). *Written statement to the 70th Session of the Commission on the Status of Women*. <https://www.soroptimistinternational.org>

Soroptimist International Australia. (2026a). *Digital safety futures: Building a cohesive national response to technology-facilitated abuse and AI-enabled harm [Policy framework and government submission]*.

Soroptimist International Australia. (2026b). *Submission to the parliamentary inquiry into intergenerational housing inequity* [Parliamentary submission].

Soroptimist International Australia. (2026c). *Submission to the inquiry into artificial intelligence and data centres* [Parliamentary submission].

Soroptimist International of Brisbane. (2026a). *Submission to the parliamentary inquiry into access to and affordability of medical specialists in Australia* [Parliamentary submission].

Soroptimist International of Brisbane. (2026b). *Shaping an equitable future: A gender-responsive blueprint for Australian employment services* [Policy submission].

Sparke Helmore Lawyers. (2025). *Serious invasion of privacy – new tort*. <https://www.sparke.com.au>

UNICEF Australia. (2024). *Social media ban in Australia: A simple guide*. <https://www.unicef.org.au>

United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development* (A/RES/70/1). <https://sdgs.un.org/2030agenda>