

Submission of Consultation to the National Plan to End Violence Against Women and Children 2022–2032

Submitted By: Francom Group

Authored By:	██████████ (Operations Executive) ██████████ (CEO, Francom Group)
---------------------	--

Email:	████████████████████
---------------	----------------------

Date:	30/07/2026
--------------	------------

Permission to publish granted

SUBMISSION THEME

Putting people, dignity and safety at the centre of every policy, service and system from the outset—so harm is anticipated and prevented, support is easier to reach, and victim-survivors remain in control.

This submission considers how a Risk of Harm Framework, trusted digital infrastructure, cyber safety principles, STEM innovation and privacy-preserving technology can be used with care to reduce harm and create safer pathways out of violence. Its purpose is to support people—not to turn their experiences into data—and to ensure every policy, service and technical decision respects dignity, autonomy, fairness and the right to be heard. The privacy-preserving technologies listed in the framework are illustrative options for further technical, legal, ethical and safety assessment; they are not endorsed solutions or direct one-to-one remedies for the corresponding sector signals.

EXECUTIVE SUMMARY

This submission proposes a people-first approach aligned with the National Plan to End Violence against Women and Children 2022–2032, including its whole-of-society focus across prevention, early intervention, response, recovery and healing. It calls for safety to be designed into policies, services, products and everyday processes from the beginning—not added after harm has occurred. Its two central proposals are:

1. a **National Trusted Support Network** that helps victim-survivors move between services without repeatedly recounting traumatic experiences, enabling coordinated and privacy-preserving support; and
2. a **National Risk of Harm Framework** that gives organisations a shared, human-centred way to recognise risk and respond with care, consistency and urgency, delivering nationally consistent responses.

Together, these proposals would reduce repeated disclosure, shorten the path to support and make organisations responsible for designing out foreseeable harm. People with lived experience should be involved throughout design, testing, implementation and review, with their time and expertise recognised. The aim is not to build technology for its own sake, but to create safer journeys in which victim-survivors understand what is happening, choose what is shared wherever possible, and can access help without having to navigate the system alone.

The current service system does not yet enable organisations to share essential risk information consistently and safely. For women and children seeking safety, fragmented processes can deepen isolation and leave the person carrying responsibility for connecting services at a time of crisis. Reform should begin by acknowledging this burden, listening to those affected and designing a pathway that offers continuity, compassion and timely help.

Privacy and identity protection are expressions of respect, not obstacles to care. Information should be shared only when necessary, lawful and safe, and in a way the person can understand. Victim-survivors should not be asked to repeatedly recount traumatic experiences across police, financial institutions, insurers, telecommunications providers, housing, health, education, legal and government services. Each retelling can cause distress, create risk and delay help. A caring system should remember responsibly so the person does not have to relive their experience to be believed or supported.

A safe system should carry the administrative burden instead of placing it on a person in crisis. Information sharing must be purposeful, limited, secure and understandable. Wherever possible, victim-survivors should decide what is shared, with whom and for how long. Where emergency action is legally required, the reasons, safeguards and review pathways should be clear.

Australia has an opportunity to redesign the support journey around the needs of victim-survivors. A trusted network could confirm essential information between authorised organisations, with informed consent wherever possible, without creating a single store of sensitive personal records. The Risk of Harm Framework would help services match their response to the person's circumstances and level of danger. Any solution should be easy to use, accessible, culturally safe, inclusive, and supported by non-digital options so no one is excluded.

ETHICS OF CARE COMMITMENTS

Across every recommendation, care should be understood as a practical duty. Organisations should listen before acting, avoid unnecessary intrusion, communicate with honesty and compassion, recognise that needs and risks change over time, and remain accountable for the consequences of their decisions. Victim-survivors should be treated as partners with knowledge of their own circumstances, not passive recipients of a system response.

Proposed ethical decision test: Before any policy, service, research project or digital feature is approved, the responsible organisation should be able to show that it meets a genuine human need; is necessary and proportionate; uses the least intrusive option; protects people who may face the greatest risk; preserves meaningful choice and human support; and provides independent oversight, explanation, correction and remedy. If these conditions cannot be demonstrated, the proposal should not proceed.

- **Dignity:** treat every person with respect and avoid language, processes or technologies that reduce them to a case, category or score.
- **Autonomy:** support informed choice and consent, including the ability to pause, change or withdraw participation wherever possible.
- **Do no further harm:** anticipate re-traumatisation, exclusion, surveillance, discrimination and misuse before a service or technology is introduced.
- **Relational care:** preserve human contact, continuity and warm referral so that no person is left to carry the system between organisations.
- **Justice and inclusion:** design for people most likely to face barriers, and provide culturally safe, accessible and non-digital pathways.
- **Transparency and remedy:** explain decisions in plain language, keep accountable people in the loop, and provide timely correction, complaint and review options.

Technology should support this approach by making safer choices easier, reducing the need to repeat information, helping authorised services coordinate quickly, and giving victim-survivors clearer control over their information and circumstances. Investment should therefore focus on practical, interdisciplinary research into safe identity checks, privacy protection, secure communication, accessible service design and responsible decision-support tools. Technology must remain an enabler of human care—not a substitute for skilled judgement, trust or face-to-face support.

This submission also proposes investment in interdisciplinary STEM research programs to build Australia's sovereign capability in secure digital identity, privacy engineering, distributed trust technologies and applied mathematics for social impact.

HOW TECHNOLOGY CAN SUPPORT A PEOPLE-FIRST SAFETY JOURNEY

Used well, technology can quietly remove friction from the support journey. It can help a person confirm essential information once, choose what each service may see, receive discreet updates through a safe channel, and move between organisations through a warm referral rather than starting again. It can also prompt trained staff when a situation may require faster support, while leaving assessment and action with accountable people.

- **Safer access:** simple identity checks and alternative pathways can reduce paperwork without excluding people who lack documents, devices or digital confidence.
- **Greater control:** clear permission settings can let a person decide what is shared, with whom and for how long, and make it easier to withdraw permission where possible.
- **Less repetition:** trusted confirmation between authorised services can reduce repeated disclosure while keeping detailed records with the organisation responsible for them.
- **Discreet communication:** safe-contact preferences, neutral notifications and quick-exit features can reduce the risk created by shared or monitored devices.
- **Faster coordination:** secure referrals and status updates can help services act together without requiring the person to coordinate every step.
- **Better staff support:** carefully tested prompts can help frontline workers recognise possible risk, but must never make final decisions or replace professional judgement.
- **Learning and accountability:** de-identified information can show where people are delayed, excluded or required to repeat themselves, allowing services to improve without creating surveillance.

Every digital feature should be tested with people who may use it under stress, on a shared device, with limited connectivity, with disability or language needs, or while being monitored. Safe defaults, minimum data collection, clear explanations, human review, independent oversight and a reliable non-digital option should be required before any technology is introduced or expanded.

RECOMMENDATION 1

ESTABLISH A NATIONAL TRUSTED SUPPORT NETWORK FOR VICTIM-SURVIVORS

Australia should establish a nationally governed way for victim-survivors to be recognised by authorised services without having to repeat traumatic details each time they seek help. The network should begin with the real support journey: what a person needs to stay safe, what makes help difficult to reach, and what choices and explanations they need at each step.

People with lived experience, specialist services and frontline workers should co-design and test the network before implementation. Victim-survivors should be able to see and understand what information is being requested, correct it, withdraw permission where possible, and choose a non-digital pathway. Organisations—not individuals in crisis—must carry responsibility for safe design, staff training, accessibility, security and timely support.

Personal information should be collected, used and disclosed transparently, securely and only to the extent necessary for a lawful purpose, with appropriate access and correction rights. Building on relevant Australian privacy requirements, this submission proposes that victim-survivors should, wherever possible, understand and control what is shared, with whom and for how long, while any emergency exception remains necessary, proportionate, documented and reviewable.

The network should support:

- secure identification and disclosure
- clear, informed and revocable consent wherever possible
- consent based sharing: sharing only what is needed for a specific purpose
- safe options for people using shared or monitored devices
- accessible, culturally safe and non-digital pathways
- auditability: the ability to review and correct information
- warm referrals and rapid access to essential services
- independent complaints, review and oversight

Participating organisations and Subject Matter Expertise could include:

- Police
- Domestic violence services
- Financial Counsellors
- Banks
- Superannuation funds
- Utility providers
- Telecommunications providers
- Insurance companies
- Medicare and health providers
- Centrelink
- Child protection agencies
- Schools
- Legal Aid
- Housing providers
- Individuals with lived experience

- Financial counselling Australia
- Leading community groups (TCA)

The network could use secure digital identity and trusted confirmations to help authorised organisations recognise that a person has already been assessed, without exposing their full history. In practice, this could allow a victim-survivor to approve a limited confirmation—such as eligibility for further support or a safe-contact preference—rather than provide the same documents and account repeatedly. Each organisation should see only what it needs for its role, every access should be recorded, and the person should have a clear way to review permissions and seek help. A staffed and non-digital pathway must always remain available.

RECOMMENDATION 2

TEST DIFFERENT WAYS TO SHARE TRUST SAFELY

Australia should test a range of approaches that allow organisations to confirm essential information without exposing a person's full history. Decisions should be led by safety, simplicity, accessibility and public benefit—not by preference for a particular technology. Each pilot should be co-designed with victim-survivors and specialist services, independently assessed for foreseeable misuse, and stopped or changed if it increases risk or confusion.

Any approach should provide:

- audit trails: a clear record of who accessed or shared information
- information integrity: proof that information has not been changed
- control over permissions and time limits
- selective disclosure of information: sharing of only the minimum necessary information
- protection against unauthorised access or tampering
- plain-language explanations and support
- safe alternatives if a person cannot or does not want to use a digital service
- consent management

Sensitive personal information should remain with the authorised organisation responsible for it and should not be copied into a shared record unless this is demonstrably necessary, lawful and safe. Any shared layer should hold only the minimum permissions and confirmation events needed to coordinate support. Informed consent should be the default. Where the law permits action without consent to prevent serious and imminent harm, the response should use the least intrusive option, be authorised by an accountable person, be recorded and reviewed, and be explained to the victim-survivor as soon as it is safe.

This keeps the focus on the person's safety and privacy while allowing services to act together, with the aim of moving a safe way forward.

RECOMMENDATION 3

REDUCE THE ADMINISTRATIVE BURDEN ON VICTIM-SURVIVORS

Administrative burden is often an invisible form of harm. Recognising financial services, utilities, and telco, and their related collections as critical safety infrastructure directly reduces administrative burden for victim-survivors. Today, women escaping violence must repeatedly verify identity, update addresses, disconnect shared accounts, restructure debt, establish financial independence and navigate hardship processes across multiple organisations. Trusted verification and nationally consistent vulnerability standards would significantly reduce repeated disclosure, accelerate access to essential financial supports and lower the emotional labour required during crisis. Women escaping violence may need to repeat the same information across numerous organisations simply to:

- prove identity
- verify circumstances
- update addresses
- disconnect shared accounts
- establish financial independence
- access emergency accommodation
- transfer utilities
- protect children's records

Every interaction demands emotional labour and time at a point when victim-survivors are already carrying the full weight of crisis, trauma and immediate caring responsibilities. A trusted verification model could allow a single verified assessment to support coordinated access across multiple organisations while preserving privacy and individual consent. This drastically lowers the threshold for accessing services during moments of vulnerability.

RECOMMENDATION 4

INVEST IN PEOPLE-LED STEM RESEARCH FOR POSITIVE SOCIAL IMPACT

The National Plan should invest in interdisciplinary STEM research that starts with the lives, priorities and rights of victim-survivors. Researchers should work alongside people with lived experience, specialist services, frontline workers and communities to define the problem, shape the research questions, test solutions in real settings and decide whether a proposed approach is safe, understandable and genuinely useful. Scientific and technical excellence should be judged not only by what can be built, but by whether it reduces harm, expands choice, improves access to support and strengthens dignity and trust.

Research should examine whether privacy-preserving methods—including selective disclosure, differential privacy, federated learning and other appropriate techniques—can support limited information sharing without creating new safety, legal or operational risks and connect each STEM capability to a clear human benefit:

- **Privacy-preserving digital identity** that helps people prove only what is necessary, without repeatedly disclosing traumatic experiences or exposing their full history.
- **Secure and discreet communication** for people using shared, monitored or compromised devices, supported by safe defaults and alternative contact pathways.
- **Accessible and culturally safe service design** that works for people with disability, diverse language and literacy needs, limited connectivity or low digital confidence.
- **Responsible artificial intelligence and decision support** that helps trained workers notice and prioritise concerns while preserving human judgement, explanation and accountability.
- **Applied mathematics and operational research** that helps services understand demand, reduce waiting and coordinate resources, without treating a person as a score or prediction.
- **Privacy-enhancing analytics** that can identify patterns of harm and service gaps without creating surveillance or unnecessary stores of personal information.
- **Human-centred systems engineering** that designs the whole support journey around safety, consent, accessibility, continuity and recovery.

- **Cyber security and resilient infrastructure** that protects sensitive information, limits access and keeps essential services available during disruption or attack.
- **Trusted digital infrastructure** that allows authorised organisations to confirm essential information and coordinate care while sharing the minimum necessary data.
- **Independent assurance and governance** that tests for misuse, bias and unintended consequences, publishes understandable findings and provides clear ways to challenge decisions.

Every research program should include lived-experience leadership, ethical and safety review, multidisciplinary expertise, staged testing and a clear pathway from evidence to practice. Non-digital options should be protected throughout. Projects should continue or scale only where independent evaluation shows positive social impact—such as fewer repeated disclosures, safer communication, shorter waits, greater understanding and control, improved access for underserved groups, stronger trust and fewer people abandoning the support process. This approach would build sovereign Australian capability while directing STEM innovation towards measurable public benefit across family and domestic violence services, health, emergency management, cyber security and government.

RECOMMENDATION 5

RECOGNISE FINANCIAL SERVICES, UTILITY, TELCO AND COLLECTIONS AS CRITICAL SAFETY INFRASTRUCTURE

Financial services, utilities, telecommunications providers and debt collection agencies may be among the first organisations to notice signs of financial abuse, coercive debt or economic control. This creates a duty to respond with care: to listen without judgement, avoid compounding distress, protect confidentiality and connect a person with appropriate support. These sectors should therefore be recognised as part of Australia's broader safety infrastructure, with trauma-informed, privacy-preserving and consent-based practices that help people reach support sooner.

Existing hardship, vulnerability and responsible-collections requirements and practices may provide a foundation for developing a nationally consistent Vulnerability and Risk of Harm Standard. Ethical practice means balancing legitimate organisational responsibilities with the dignity, safety and circumstances of the person. It requires patient communication, flexible processes, trained staff, strong governance and technology that supports compassionate service rather than creating distance. These practices can inform national guidance and cross-sector learning.

Government and industry should work together to:

- embed Safety by Design obligations into financial products and collections
- enable consent-based trusted verification across regulated sectors
- recognise financial abuse indicators within the National Risk of Harm Framework
- support cross-sector pilots measuring reductions in harm, repeated disclosure and time to support

Recognising financial services as critical safety infrastructure ensures regulated industries become active participants in reducing harm, improving safety and accelerating recovery.

DEVELOP A NATIONAL CROSS-SECTOR TRUST AND CARE FRAMEWORK

Technology alone cannot repair fragmented service delivery. Australia needs shared governance that turns trust, care and accountability into everyday practice. The framework should make clear who is

responsible for the person's experience, how dignity and consent will be protected, and what remedy is available when care falls short. It should establish:

- shared standards for safe and respectful verification
- consent and supported decision-making arrangements
- clear privacy, confidentiality and data-minimisation duties
- interoperability that supports continuity of care
- proportionate cyber security and resilience standards
- accreditation, training and wellbeing support for participating organisations and staff
- named responsibility for decisions and service failures
- independent oversight, accessible complaints and meaningful remedy

A nationally recognised trust framework would give banks, financial services, insurers, utility providers, telecommunications providers and government agencies a secure, privacy-preserving way to collaborate, meet their regulatory obligations and mobilise rapid, coordinated support that helps women and children leave violent situations safely.

RECOMMENDATION 6

EARLY SUPPORT THROUGH SAFE AND LIMITED INFORMATION SHARING

With clear legal authority, strong safeguards and informed consent wherever possible, technology may help authorised services recognise circumstances that warrant a safe and supportive check-in. A signal is not proof of violence, a judgement about credibility or a reason for punishment. It should prompt a trained worker to consider context, check for error or bias, use the person's safe-contact preferences, and offer choices about support. Relevant circumstances may include:

- repeated changes of address
- sudden financial distress
- emergency hardship requests
- rapid utility account transfers
- police referrals
- court protection orders
- domestic violence support referrals

Rather than automatically combining personal records, services could use limited and purpose-specific confirmations to support earlier action. Alerts should be visible only to authorised staff, expire when no longer needed, be checked for error or bias, and lead first to a safe offer of support. Emergency responses should occur only where lawful and necessary, with clear accountability and review.

The emphasis must remain on safeguarding and supporting people—not monitoring them. No person should lose access to a service, face an adverse decision or be referred to enforcement solely because of an automated signal.

RECOMMENDATION 7

PURPOSE AND INTENDED OUTCOME OF THE RISK OF HARM FRAMEWORK

Develop a national, cross-sector risk-of-harm framework that helps people and organisations recognise technology-facilitated abuse, coercive control, financial harm and escalating danger. Technology can support the framework by presenting consistent questions, recording the person's preferences, highlighting relevant information for trained staff and coordinating agreed actions. It must not replace conversation, professional judgement or the victim-survivor's own understanding of risk.

Financial abuse can contribute to entrapment, coercive control and prolonged exposure to violence. Indicators of financial harm may include coercive debt, repeated hardship requests, unusual payment activity, forced account changes, identity misuse, utilities transferred under duress and vulnerability markers observed within debt collection processes.

Integrating financial harm into the national taxonomy ensures that regulated industries identify and classify risk consistently, enabling proportionate, privacy-preserving and consent-based responses. This strengthens early intervention pathways and supports nationally coordinated action across banks, creditors, utilities, telecommunications providers and collections agencies.

Core ethical and safety principles: care and dignity first; prevention of further harm; informed choice and supported autonomy; necessity and proportionality; least intrusive, most protective response; privacy, security and safety by design; fairness and cultural safety; accountable human judgement; transparency and explainability; contestability, independent oversight and meaningful remedy.

Scope of Harm: Technology-Facilitated Abuse, Coercive Control, Escalating Physical/Psychological Risk, Financial Harm

CROSS-SECTOR SIGNALS		PRIVACY-PRESERVING DESIGN
Telecommunications: SIM swaps, account takeover, tracking		Zero-Knowledge Proofs
Financial Services: coercive debt, forced transfers		Differential Privacy
Digital Platforms: harassment, impersonation, image abuse		Consent-Based Release
Government Services: unsafe contact, repeated disclosure		Federated Learning
Health/Education/Housing: behavioural escalation		Unsafe home
NATIONAL RISK TAXONOMY (4 LEVELS) <i>This submission proposes a four-level national risk taxonomy as a starting point for consultation. The taxonomy would use consistent definitions, categories and language so participating agencies can describe comparable risks consistently, reduce the chance that signals are lost or misinterpreted, support appropriate comparison or aggregation of information, improve cross-sector coordination, and promote more consistent responses for victim-survivors. The model should be validated with specialist services, lived-experience leaders, researchers, regulators and participating sectors before adoption.</i>		
LEVEL	RISK	ESCALATION PATHWAYS
1	Early Indicators: subtle digital red flags, unusual activity	Early alerts → privacy-preserving prompts to seek support
2	Emerging Risk: escalating surveillance, financial control	
3	High Risk: explicit threats, forced access, stalking	Coordinated response → authorised agencies receive verified signals
4	Critical / Imminent Harm: real-time threats, active tracking	Rapid safety action → immediate cross-sector intervention Victim-Survivor Control → consent determines who receives information
GOVERNANCE		
- National Standards Body - Regulated Industry Duties - Audit & Transparency		

- Independent Oversight

RECOMMENDATION 7

PROPORTIONALITY IN IMPLEMENTATION

To create a nationally consistent way to recognise and respond to escalating harm while preserving care, context and human judgement. Its purpose is not simply to move information faster, but to help the right people offer the right support at the right time. A proportionate response should reduce repeated disclosure, protect privacy, explain what is happening and keep the victim-survivor's wishes central wherever possible. The measure of success is whether people feel safer, heard and supported—not merely whether a process has been completed.

RECOMMENDATION 8

ETHICAL NATIONAL IMPLEMENTATION

National implementation should be treated as a public-interest and duty-of-care program, not simply a technology rollout. A nationally consistent model should establish shared ethical duties while allowing implementation to respond to local laws, communities, service systems and cultural contexts. Progression from design to pilot and national scale should occur only where there is evidence that the model is safe, lawful, effective, proportionate and trusted by victim-survivors. No jurisdiction or participating organisation should lower these safeguards in the interests of speed, cost or technical convenience.

NATIONAL ETHICS AND SAFETY GOVERNANCE

The Australian Government should establish an independent national ethics and safety council to govern implementation across the Commonwealth, states and territories. Its membership should include remunerated lived-experience representatives, Aboriginal and Torres Strait Islander leadership, culturally and linguistically diverse communities, disability advocates, specialist domestic and family violence services, privacy and human-rights experts, frontline practitioners, cyber-security and digital identity specialists, researchers, regulators and participating service sectors. The council should publish binding minimum safeguards, approve pilots, monitor national consistency, disclose conflicts of interest, receive independent assurance reports and have authority to pause, modify or stop implementation where harm or unacceptable risk emerges.

- **Commonwealth, state and territory governments** to align legislation, funding, service standards and accountability.
- **Specialist domestic and family violence organisations and lived-experience leaders** to hold decision-making roles throughout design, testing and review.
- **Financial institutions, telecommunications providers, utilities, insurers and government services** to meet common duties of care, consent, privacy, accessibility and safe referral.
- **Privacy, human-rights, safety and sector regulators** to provide coordinated oversight without weakening existing protections.
- **Universities, Standards Australia, cyber-security experts and digital specialists** to support independent research, assurance and interoperable standards.

- **Community-controlled and place-based organisations** to ensure implementation is culturally safe, accessible and responsive to local conditions.

Before any national implementation, the pilot should be independently evaluated against ethical, safety and public-interest criteria, including:

- **Safety and prevention of harm:** whether the model reduces risk, avoids re-traumatisation and identifies any new or unequal harms before they are scaled nationally.
- **Dignity, autonomy and consent:** whether people understand the process, retain meaningful choice, can withdraw where possible and have access to supported and non-digital pathways.
- **Equity and cultural safety:** whether the model works fairly for Aboriginal and Torres Strait Islander peoples, culturally and linguistically diverse communities, people with disability, children and young people, and people in regional, rural and remote communities.
- **Privacy and information stewardship:** whether collection and sharing are lawful, purpose-limited and proportionate, use the minimum necessary information, and provide access, correction and clear retention limits.
- **Human accountability and remedy:** whether consequential decisions remain with trained and accountable people, and whether explanations, complaints, review, correction and redress are accessible and timely.
- **Service experience and wellbeing:** whether the model reduces repeated disclosure and access times, improves safe referrals, supports wellbeing and strengthens trust without shifting administrative burden onto victim-survivors.
- **Security, resilience and interoperability:** whether the system can operate safely across jurisdictions and sectors, withstand misuse or disruption, and exchange only authorised information under nationally consistent safeguards.
- **Proportionality and public value:** whether demonstrated human and social benefits outweigh foreseeable risks and costs; efficiency savings should be treated as secondary to safety, rights and equitable access.
- **Readiness to scale:** whether independent assurance, workforce capability, sustainable funding, local adaptation, transparent reporting and national oversight are in place. National expansion should proceed in stages and may be paused, changed or stopped if ethical or safety thresholds are not met.

ETHICAL CROSS-SECTOR DESIGN AND BROADER PUBLIC BENEFIT

The proposed trusted infrastructure should be designed as a common ethical foundation that can support different sectors without imposing a single, rigid operating model. Its shared purpose would be to help organisations verify essential information, coordinate timely support and reduce repeated disclosure while preserving dignity, consent, privacy, fairness and human judgement. Each sector should adopt the same minimum safeguards but tailor workflows, professional responsibilities and escalation pathways to its legal obligations, service context and the needs of the people it serves.

A cross-sector implementation model should combine:

- **A common ethical core:** dignity, supported autonomy, prevention of harm, fairness, cultural safety, accessibility, privacy, transparency and meaningful remedy.
- **Shared technical foundations:** secure identity, minimum necessary disclosure, interoperable standards, resilient cyber security, auditable access and safe consent management.
- **Sector-specific safeguards:** controls and service pathways suited to finance, telecommunications, utilities, insurance, health, education, housing, justice, government and community services.
- **Accountable human decisions:** technology may verify, prompt and coordinate, but trained people remain responsible for consequential decisions and communication.
- **Independent assurance:** privacy, safety, human-rights and accessibility assessments before implementation, followed by continuing monitoring, transparent reporting and external review.
- **Safe participation and choice:** clear explanations, non-digital options, correction and withdrawal pathways, and no loss of essential service for declining a digital process.

Subject to these safeguards, the model could be adapted for disaster recovery, homelessness and housing support, veterans' services, disability services, child protection, refugee settlement, aged care and health care coordination. Expansion should occur only where a sector has demonstrated a genuine public-interest need, consulted affected communities, defined lawful and limited information flows, trained accountable staff, and shown through independent evaluation that benefits outweigh foreseeable risks. Organisational efficiency or cost savings may be considered, but they must never displace safety, rights or equitable access as the primary measure of success.

This submission draws on publicly available Australian policy, regulatory and guidance materials, including the National Plan to End Violence against Women and Children 2022–2032, the eSafety Commissioner's Safety by Design guidance, the Australian Privacy Principles and human-rights guidance on automated decision-making. Before publication, every quotation, close paraphrase, established framework, distinctive term and factual or legal claim derived from these materials should be identified in the text and included in a complete reference list. Material developed specifically for this submission should be clearly distinguished from sourced concepts and language.

CONCLUSION

Ending family and domestic violence against women and children requires ethical, system-wide change that places dignity, safety, autonomy and care at the centre of every policy, service, product and decision. Australia should move beyond responding after harm occurs and embed Safety by Design across government, regulated industries, community services and digital systems, so foreseeable risks are prevented, organisations act together and the burden of navigating fragmented support no longer rests with victim-survivors. Guided by lived experience and supported by accountable human judgement, responsible STEM research and privacy-preserving technology, this approach can create safer, more accessible and coordinated pathways for women and children experiencing violence and for all victim-survivors—while ensuring innovation is measured by its capacity to reduce harm, strengthen choice, build trust and support recovery.

An ethically governed, privacy-preserving support network should form part of a broader transformation in how governments, regulated industries and community services prevent and respond to family and domestic violence. Built on Safety by Design, strong cyber security, minimum necessary disclosure and clear public-interest governance, it should reduce administrative burden, minimise repeated disclosure

of traumatic experiences and improve coordinated access to essential services for women and children experiencing violence and for all victim-survivors. Technology may verify, prompt and connect, but trained and accountable people must retain oversight of every consequential assessment, disclosure, escalation and decision, with accessible explanation, review, correction and remedy.

Targeted interdisciplinary STEM investment should advance this ethical and system-wide change, not technology for its own sake. Research and implementation should be co-designed with remunerated lived-experience leaders, specialist services, frontline practitioners and affected communities, and should strengthen Australia's sovereign capability in secure digital identity, privacy engineering, trusted information sharing and responsible decision support. Every initiative should be independently assessed for necessity, proportionality, accessibility, cultural safety, foreseeable misuse and unequal impacts, and should proceed only where evidence shows that it improves safety, autonomy and access while preserving meaningful human support and oversight.

By embedding ethics, care and Safety by Design across policy, services, products and digital systems, the National Plan can shift responsibility for preventing foreseeable harm from victim-survivors to the organisations that design and deliver support. Success should be measured in human terms: fewer repeated disclosures, shorter waits, safer communication, greater understanding and control, more effective warm referrals, fewer people abandoning the process, and stronger trust in services. Technology should remain an enabler of compassionate, coordinated practice—not a substitute for professional judgement or human connection—and should be expanded only where continuing independent evaluation confirms that it reduces harm without creating new risks; where those thresholds are not met, implementation must be changed, paused or stopped.

Further Recommendations on Safety by Design, operational threat intelligence, responsible artificial intelligence and national innovation capacity

The following recommendations extend the submission's people-first approach to Safety by Design, cyber-threat modelling, technology-facilitated abuse, platform accountability and operational intelligence.

RECOMMENDATION 9

SAFETY BY DESIGN

Drawing on the eSafety Commissioner's Safety by Design principle of service provider responsibility, providers should carry primary responsibility for anticipating and addressing foreseeable safety risks rather than placing that burden on people seeking help.

RECOMMENDATION 10

OPERATIONAL THREAT INTELLIGENCE

Adapt cyber-security threat modelling cautiously to help frontline organisations understand how services and technologies may be misused in family and domestic violence. Models should support prevention and preparedness, not profile victim-survivors or treat behavioural patterns as proof. Any operational use should be purpose-limited, independently tested, subject to human review, and linked to a supportive and proportionate response.

RECOMMENDATION 11

RESPONSIBLE AI

Fund responsible artificial intelligence and decision-support research only where it addresses a clearly defined human need. Systems should be co-designed with victim-survivors and frontline services, use the minimum necessary information, explain what influenced a prompt, be tested for bias and misuse, and keep a trained person accountable for every consequential decision. Technology should help staff notice, prioritise and coordinate; it should never determine credibility, deny support or replace direct engagement.

RECOMMENDATION 12

NATIONAL INNOVATION HUB

Create an interdisciplinary innovation hub bringing together government, universities, industry, cyber-security specialists, specialist family and domestic violence organisations and remunerated lived-experience advisers. The hub should operate under an independent ethics and safety charter, disclose conflicts of interest, assess projects before and during trials, protect participants from re-traumatisation or exclusion, publish understandable findings, and stop or redesign any pilot where evidence of harm outweighs benefit.

ADDITIONAL STEM RESEARCH PRIORITIES

- Technology-facilitated abuse detection and measurement.
- Mathematical models for coercive control and behavioural indicators.
- Privacy-preserving digital identity and blockchain-enabled trust networks.
- Board-level operational risk reporting for emerging digital harms.
- Safety-by-Design assurance frameworks for AI and digital services.

REFERENCES

Australian Government, Department of Social Services. (2022). *National Plan to End Violence against Women and Children 2022–2032: Ending gender-based violence in one generation*. Commonwealth of Australia. Published 17 October 2022. ISBN 978-1-921130-37-3. Licensed under Creative Commons Attribution 4.0 International.

eSafety Commissioner. (2019). *Safety by Design Principles: Placing user safety at the forefront of online service design*. Office of the eSafety Commissioner. The principles address service provider responsibility, user empowerment and autonomy, and transparency and accountability.

eSafety Commissioner. (2026). *Safety by Design*. Australian Government. Updated 8 January 2026. Web guidance on embedding user safety and rights in the design and development of online products and services.

eSafety Commissioner. (2026). *Safety by Design foundations*. Australian Government. Published 6 March 2026. Practical guidance for identifying, mitigating and responding to online harms through organisational culture, policies, product features and design.

Office of the Australian Information Commissioner. (2026). *Australian Privacy Principles Guidelines: Privacy Act 1988*. Combined May 2026. Initial publication February 2014. Commonwealth of Australia. Licensed under Creative Commons Attribution 3.0 Australia.

Commonwealth of Australia. (1988). *Privacy Act 1988* (Cth), including Schedule 1, Australian Privacy Principles, as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth). The Australian Privacy Principles took effect on 12 March 2014.

Australian Human Rights Commission. (2021). *Human Rights and Technology: Final Report*. Australian Human Rights Commission. ISBN 978-1-925917-30-7. Licensed under Creative Commons Attribution 3.0 Australia.

Australian Human Rights Commission. (2025). *Use of Automated Decision-Making by Government*. Submission to the Attorney-General's Department, 15 January 2025. Australian Human Rights Commission.

Australian Human Rights Commission. (2020). *Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias—Technical Paper*. Australian Human Rights Commission. ISBN 978-1-925917-27-7. Licensed under Creative Commons Attribution 4.0 International.

Australian Government, Department of Industry, Science and Resources. (2019). *Australia's AI Ethics Principles*. Published 7 November 2019; updated 2 December 2025. Australian Government.

Digital Transformation Agency. (2023). *Digital Service Standard 2.0*. Australian Government. Launched December 2023; mandatory for new public- and staff-facing Australian Government digital services from 1 July 2024 and fully in effect for existing public-facing services from 1 July 2025.

Australian Signals Directorate. (2026). *Information Security Manual*. Australian Cyber Security Centre, Australian Government. June 2026 release. A risk-based cyber-security framework for protecting information technology and operational technology systems.

National Institute of Standards and Technology. (2025). Near, J., Darais, D., & Lefkowitz, N. *Guidelines for Evaluating Differential Privacy Guarantees*. NIST Special Publication 800-226. U.S. Department of Commerce. Published 6 March 2025. DOI: 10.6028/NIST.SP.800-226.

National Institute of Standards and Technology. (2024). Near, J., & Darais, D. *Protecting Trained Models in Privacy-Preserving Federated Learning*. NIST Cybersecurity Insights, 15 July 2024. Part of the NIST–United Kingdom Responsible Technology Adoption Unit series on privacy-preserving federated learning.