2025 Digital ID Rules and Accreditation Rules Consultation Submission

The Social Policy Group

September 2025

About The Social Policy Group

The Social Policy Group (SPG) is a trusted partner of government, community leaders and service providers with a proven track record of delivering impactful and responsive social policy solutions for Australia's communities. As a peak body for settlement, multicultural health, and multicultural affairs, and a recognised leader in best practice and thought leadership across areas such as gender equality, economic analysis, access to justice, and community sector capacity building. SPG plays a pivotal role in fostering equitable social policies through facilitation, evidence-based practice, and collaborative partnerships.

SPG is a leading national voice in social policy with deep expertise across:

- Gender equality and women's economic security
- Health equity and access
- Settlement and migration policy and capacity building
- Justice and community safety
- Artificial intelligence and digital policy
- Social cohesion and multicultural affairs
- Strengthening responses to and understanding of mis- and dis-information

Background

SPG was engaged by Services Australia National Multicultural Advisory Group communication to provide insights and feedback on the redress framework in the 2025 Digital ID Rules and Accreditation Rules Consultation. SPG welcomes this opportunity.

SPG recognises that the Department of Finance is seeking feedback on proposed amendments to the Digital ID Rules and the Accreditation Rules. SPG acknowledges that these amendments were developed following previous rounds of public consultations on Digital ID Rules, Accreditation Rules and Data Standards consultations. Because SPG was not engaged to provide feedback in those earlier rounds, SPG hopes that this submission will help strengthen the overall reform process by providing fresh perspectives.

From the document shared with SPG by Services Australia National Multicultural Advisory Group communication, SPG understands that Department of Finance is seeking feedback on the following key areas:

1. Requirements for entities to consider notifying individuals affected by cyber security or fraud incidents.
2. Obligations to publish clear policies for incident management and complaints handling, with a six-month transition period.
3. A 28-day timeframe for referring unresolved issues to the System Administrator.
4. A proposed seven-year consent duration for business-related services.
5. Support for individuals without standard ID documents through alternative proofing pathways.
6. Potential future arrangements allowing trusted nominees to act on behalf of others.

To access information, SPG assessed Department of Finance *Consultation guide: Proposed amendments to the Digital ID Rules and the Digital ID (Accreditation Rules)*. SPG realises that the alternative proofing pathways for individuals without standard ID documents and the potential future arrangements allowing trusted nominees to act on behalf of others are not covered in the consultation guide. SPG also recognises that a proposed seven-year consent duration for business-related services may not be applicable for the migrant and refugee cohort. Therefore, these three topics are discussed separately as additional recommendations outside the consultation questions in the consultation guides first in this document. SPG's feedback on requirements for entities to consider notifying individuals affected by cyber security or fraud incidents, obligations to publish clear policies for incident management and complaints handling, and a 28-day timeframe for referring unresolved issues to the System Administrator is provided in the following section titled *Consultation Guide Questions*.

In this submission, SPG provides feedback on the proposed amendments to the redress framework, centring the experiences of migrants, refugees, and minority, marginalised, and vulnerable communities, because these groups face unique challenges.

Additional Recommendations Outside the Consultation Questions in the Consultation Guide:

SPG recognises that in 2024, the Department of Finance worked with inclusion experts to develop a more inclusive Digital ID System. SPG understands that this led to initiatives including:

- Continued efforts to reduce barriers for people to get and refuse a Digital ID if they choose from resources.
- Exploration of ways to broaden the range of ID documents that can be used to create a Digital ID, including testing alternative proofing mechanisms such as digital vouching.
- Development of inclusive communications, including:
  - The Digital ID Handbook, which helps to address barriers of digital ability.
  - Easy Read content to support accessibility.

- Translated support materials for culturally and linguistically diverse communities.
- Short-form videos, with transcripts, to explain key concepts in a clear and engaging way.

SPG welcomes these initiatives to make the Digital ID System more inclusive, and strongly supports the need to broaden the range of ID documents and develop resources that ensure equitable access for all community members.

On support for individuals without standard ID documents through alternative proofing pathways:

SPG recognises the genuine need to broaden the types of identity documents that can be registered in myID by migrants, refugees and temporary visa holders, and considers support for individuals without standard ID documents through alternative proofing pathways essential.

Under the current framework, non-permanent visa holders can only strengthen their identity level in myID to a certain level. This possibility is amplified if the access of identity documents was restricted in the home country, especially for members from the refugee background. Without broadening the types of identity documents, they will continue to face barriers to accessing entitled government services.

SPG recommends that alternative proofing pathways must prioritise safety, protection and individual choice, and must be genuinely accessible. Migrants, refugees and temporary visa holders are particularly vulnerable if such pathways do not ensure the safety and privacy of their identity documents, or if access is restricted by factors such as English language proficiency.

Due to the limited detail on alternative proofing pathways in the consultation guide, SPG would welcome further information to provide evidence-based feedback from its extensive community engagements.

On potential future arrangements allowing trusted nominees to act on behalf of others:

SPG recognises that situations where an individual asks a trusted nominee to act on behalf, or to assist them in accessing government services, can occur, particularly for people facing barriers such as low English proficiency or digital literacy. However, SPG stresses the importance of recognising the risks, including situations where a trusted nominee may perpetrate harm, such as in cases of domestic and family violence.

Given the absence of implementation detail in the consultation guide, SPG would welcome further information on how trusted nominees will be confirmed, the scope of services they can access, and how the individual's ongoing consent and safety will be assured.

On proposed seven-year consent duration for business-related services:

SPG notes the proposed amendment creates a separate expiry period of 7 years when the individual declares that they are using an Attribute Service Provider's accredited services for or on behalf of a business (including a business they personally operate). The 7-year consent timeframe applies to accredited Attributed Service Providers only and, currently, the only accredited Attribute Service Provider is the Australian Tax Office (ATO), which provides a service known as the Relationship Authorisation Manager (RAM).

SPG emphasises that individuals from migrant and refugee backgrounds may face barriers in linking to RAM under the current rules. Currently, linking a principal authority's business requires a Strong identity strength, or at least Standard identity strength via alternative methods outside myID.[1] A Strong identity strength can only be achieved with an Australian passport that is current or no more than three years expired.[2] These limitations risk excluding some individuals from accessing RAM through digital ID.

Consultation Guide Questions:

Consultation Question 1. Considering whether it is appropriate to notify an individual: do the proposed factors to consider in relation to whether it is appropriate to notify an individual strike the right balance between user protection and security risks?

Recommendations:

- Consideration should be in favour of notification when identity documents or other high-risk information are exposed.
- Oversight mechanism is needed to ensure that any decision not to notify individuals is subject to independent oversight, with entities required to justify their reasoning.
    - A sensible timeframe of hearing must be established due to the potential level of harm that can occur as a result of cyber security incident or digital ID fraud.
- Provide clear guidance on what constitutes 'harm'. This must be aligned with the Privacy Act's broad test.
- Explicitly recognise that migrants, refugees and minority, marginalised, and vulnerable communities may face disproportionate risks.

SPG notes that the proposed amendments require Identity Service Providers and Attribute Service Providers participating in the Australian Government Digital ID System to consider the following factors while assessing if individuals should be notified:

---

[1] Relationship Authorisation Manager, *Set up your Digital ID and identity strength*, Relationship Authorisation Manager, accessed 26 September 2025, https://info.authorisationmanager.gov.au/link-to-a-business-in-ram/set-up-your-digital-id-and-identity-strength.
[2] myID, *How to set up myID*, myID, accessed 26 September 2025, https://www.myid.gov.au/how-to-set-up-myid#myid-Identitystrength.

- The likelihood of harm to the individual, and
- The potential impact on the operation of the Australian Government Digital ID System.

SPG considers the proposed amendments a sensible starting point for balancing user protection with broader system security. However, protection of individual users should be prioritised.

Australian law requires organisations covered by the Privacy Act 1988 to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) of a data breach if there has been unauthorised access to, or disclosure of, personal information, and it is likely to result in serious harm.[3] In making the assessment of the likelihood of serious harm, entities must consider a range of factors, including the type and sensitivity of the information, whether it is protected by security measures (for example, encrypted), the kinds of people who could access the information, and the nature of the potential harm.[4] It is necessary to clarify that both Identity Service Providers and Attribute Service Providers accredited to participate in the Australian Government Digital ID System are subject to the Privacy Act 1988.[5]

It is important to note that while identity documents are technically classified as personal information rather than 'sensitive information' under Section 6 (1) of the Privacy Act, the OAIC's guidance indicates that breaches involving identity documents often give rise to a likelihood of serious harm, and therefore frequently result in notification under the Notifiable Data Breaches (NDB) scheme.[6] This is because identity documents can readily be misused for identity theft, fraud, or to access government and financial services. Therefore, although the Privacy Act does not mandate automatic notification where identity documents are involved, OAIC guidance treats such documents as inherently higher risk. In practice, breaches involving identity documents commonly support a finding that serious risk is likely and thus often lead to notification under the NDB scheme.

---

[3] Office of the Australian Information Commissioner, *Part 4: Notifiable Data Breach (NDB) Scheme*, Office of the Australian Information Commissioner website, accessed 26 September 2025, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme.

[4] Office of the Australian Information Commissioner, *Part 4: Notifiable Data Breach (NDB) Scheme*.

[5] Office of the Australian Information Commissioner, *Interaction between the Digital ID Act and the Privacy Act*, Australia's Digital ID System, accessed 26 September 2025, https://www.digitalidsystem.gov.au/digital-id-accreditation/privacy-materials-for-accredited-entities/interaction-between-the-digital-id-act-and-the-privacy-act.

[6] Australian Law Reform Commission, *Sensitive information*, Australian Law Reform Commission, accessed 26 September 2025, https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/6-the-privacy-act-some-important-definitions/sensitive-information/; Australian Law Reform Commission, *What is 'personal information'?*, Australian Law Reform Commission, accessed 26 September 2025, https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/6-the-privacy-act-some-important-definitions/what-is-personal-information; Office of the Australian Information Commissioner, *Notifiable Data Breaches scheme 12-month insights report*, Office of the Australian Information Commissioner, accessed 26 September 2025, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-scheme-12-month-insights-report.

By contrast, the proposed amendments only require providers to consider whether notification is 'appropriate.' This risks inconsistency with the Privacy Act and creates the possibility that individuals will not be notified even where serious harm is likely. The introduction of 'impact on the operation of the system' as a counter-factor magnifies this risk, as entities may prioritise system stability over user protection.

This problem is particularly acute for migrants, refugees and people from vulnerable backgrounds, who may face disproportionate harm from identity fraud due to precarious visa status, past experiences in home countries (especially for refugees fleeing war or persecution), language abilities, and accessibility to government services to quickly replace compromised documents or issues. For these groups, delayed or absent notification could have serious consequences.

Consultation Question 2. Published incidents policies: are there any minimum requirements that the policies relating to the identification, management and resolution of incidents should contain, that would not exacerbate harm?

Recommendations:

- Clear standards need to be mandated to strike the right balance between the amount of information that should be included in the published policies so that the policies provide sufficient information to users while also safeguard the system security.
- Policies should be written in easy English and translated to appropriate community languages where possible.

SPG recognises that the proposed amendments will introduce an obligation for Identity Service Providers and Attribute Services Providers participating in the Australian Government Digital ID System to publish policies that explain how they identify, manage, and resolve cyber security and digital ID fraud incidents.

SPG welcomes this amendment because it can promote transparency and accountability. Transparency and accountability are crucial in enhancing public confidence in government services. More importantly, individuals have a right to understand how their data will be safeguarded and what steps will be taken if an incident occurs.

Nevertheless, SPG would like to stress the need to develop clear standards on how much information needs to be included in the published policies. Without clear standards, on the one hand, there is a risk that entities will publish generic information that does not meaningfully inform individuals or provide assurance. On the other hand, there is a risk of providing malicious actors with intelligence on system defences if the policies contain overly detailed disclosure.

To strike the right balance, the standards should require the policies to:

- Clearly outline what individuals can expect if their identity documents are compromised.

- Demonstrate how the Identity Service Providers and Attribute Services Providers comply with the NDB scheme.
- Provide practical and timely information about available support services and necessary next steps to individuals after an incident.

Whether the access to these policies is equitable is especially critical for migrants, refugees, and minority, marginalised, and vulnerable communities, as they may face greater challenges in navigating cyber incidents and accessing remedies. It is, therefore, critical that the policies are transparent, accessible, and user centred. SPG recommends that policies be written in easy English to ensure greater outreach and be translated into appropriate community languages where possible.

Consultation Question 3. Published complaints handling policies: are the minimum requirements for the complaints policies satisfactory?

Recommendations:

- Strike the right balance between knowledge and responsibility to ensure individual users are sufficiently notified for digital ID fraud and cyber security incidents, while avoiding situations where users are overburdened with the responsibility of detecting such incidents in order to make a complaint.
- Develop reasonable timeframes for resolving complaints to ensure public trust in the complaints system, and to allow visa holders sufficient opportunity to seek an appropriate level of remedy.
- Complaint policies must be written in easy English to ensure broad accessibility and should be translated into appropriate community languages where possible.
- Where entities' existing complaints handling policies are not related to identity documents, complaints policies for digital ID should be developed separately, in recognition of the greater magnitude of harm associated with identity document fraud and cyber security incidents.

SPG recognises that the proposed amendments will introduce an obligation for Identity Service Providers and Attribute Services Providers participating in the Australian Government Digital ID System to develop and publish clear complaints policies. These policies must explain how individuals affected by digital ID fraud and cyber security incidents can make a complaint if something goes wrong, and what to expect once a complaint is made.

SPG welcomes this amendment because it promotes transparency and accountability. Individuals using the Australian Government Digital ID System are entitled to the right to make complaints. This right is supported within the framework of Digital ID Act. Therefore, it is reasonable that Identity Service Providers and Attribute Services Providers develop and publish clear complaints policies that guide individuals affected by digital ID fraud and cyber security incident in making a complaint.

However, SPG sees the need to carefully balance knowledge and responsibility. As the proposed amendments on complaints handling specifically address cases of digital ID fraud and cyber security incidents, it is reasonable to assume that individual complaints may arise from two channels:

1. Individual users detect digital ID fraud or cyber security incidents and initiate the complaints process.
2. Individual users initiate complaints process as a result of being notified by entities of digital ID fraud and cyber security incidents.

If the amendments lean heavily on the first scenario, individual users may be left carrying an unreasonable burden in the complaints process. First, individuals are unlikely to have the knowledge or access required to detect digital ID fraud or cyber security incidents. Second, if individual users do manage to identify incidents, the harm is already likely to have occurred.

If the amendments are designed around the second scenario, it becomes imperative to lower the threshold for notifying individual users about digital ID fraud and cyber security incidents. In this case, the balancing act in Requirement 1, between the need to notify users and the security of the system, would be incompatible with this amendment, unless individuals' likelihood or ability to make a complaint is itself considered a factor. If this is the case, then notification is almost always required.

Whether the right balance is stuck and whether the complaints policies are equitable is especially critical for migrants, refugees, and minority, marginalised, and vulnerable communities. These groups can face greater barriers in navigating complaint processes. It is also important to establish reasonable timeframes for resolving complaints. On one hand, reasonable timeframes can increase users' trust in the system. On the other hand, many visa holders cannot realistically pursue a prolonged complaints process. If complaints cannot be resolved within a reasonable timeframe, some cohorts of digital ID users will suffer greater harm from fraud or cyber security incidents simply because they lack permanent residency in Australia.

It is also essential that complaints policies are transparent, accessible, and user centred. SPG recommends that policies be written in easy English, and translated into appropriate community languages where possible.

Finally, SPG sees a potential need to separate complaints policies related to digital ID fraud and cyber security incidents from other complaints handling policies used for unrelated services. This is because the magnitude of harm from identity fraud and related cyber incidents far outweighs other types of harm.

Consultation Question 4. Escalation to the System Administrator: is the proposed escalation timeframe (within 28 days) sufficient to ensure timely resolution of unresolved user issues?

Recommendations:

- A shorter timeframe should be adopted given the potential harms that can result from unresolved digital ID and cyber security incidents.
- The 28-day limit should act as an absolute outer boundary for all cases, as opposed to only cases raised through complaints.
- Entities must provide clear communication to individuals about expected timeframes, progress updates, and next steps to reduce uncertainty and frustration.
- Referrals to 'public resources' or 'other entities' must not place the burden on individuals to resolve their own cases and must not prolong the referral of the cases to the System Administrator beyond the 28-day timeframe. Entities should retain responsibility and actively case-manage issues until resolution.
- Migrant, refugees, temporary visa holders and other marginalised users are disproportionately harmed by delays and cross-referrals. Escalation standards should reflect these risks by ensuring timeliness and accessibility.

SPG recognises that the proposed amendments will introduce an obligation for Identity Service Providers and Attribute Service Providers participating in the Australian Government Digital ID System to refer unresolved technical issues to the System Administrator. This obligation will apply even if the issue does not involve other services in the system. Referrals must be made as soon as reasonably practicable and, if linked to a complaint, within 28 days.

SPG welcomes this reform as it formalises existing guidance and ensures that individuals are not left without a pathway to resolution. By strengthening accountability, the amendment has the potential to increase public confidence in the system's ability to respond to complex or unresolved issues.

However, SPG is concerned that the 28-day timeframe can potentially be too long to adequately protect users. For digital ID fraud and cyber security incidents, delays in escalation can result in significant harm, including identity theft, financial loss, and barrier to accessing essential services. For visa holders, unresolved issues may also affect their legal status or employment rights, creating particularly acute risks if resolution is delayed.

SPG therefore recommends clarifying that referrals must occur as soon as reasonably practicable, with 28 days only serving as an upper limit. Entities should also provide users with clear communication about why the matter is being escalated, what steps the System Administrator may take, and what outcomes and timeframes can be expected.

SPG also notes that amendment's requirement that entities must be 'reasonably satisfied' that an issue cannot be resolved without referral, and that they must assist individuals by directing them to

public resources or other entities. While SPG acknowledges that this is well intentioned, this could carry a risk that responsibility is shifted to victims who may be left to navigate fragmented referral pathways at a time of stress. Additionally, cross referrals might also create a risk of prolonging the timeframe to escalate the issue to System Administrator, resulting in more harms.

Migrants, refugees, and people with limited English or digital literacy are particularly vulnerable in these circumstances. Entities must retain responsibility for managing the issue until it is resolved, and any referral to other entities should be actively facilitated rather than delegated to the individual.

SPG highlights that migrants, refugees, and minority, marginalised, and vulnerable communities are disproportionately impacted by delays and cross referrals. For these groups, the inability to resolve identity document or access issues can result in long-lasting consequences. Therefore, escalation standards should reflect these risks to ensure timeliness, accountability, and equitable access.

References

Australian Law Reform Commission, *Sensitive information*, Australian Law Reform Commission, accessed 26 September 2025, https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/6-the-privacy-act-some-important-definitions/sensitive-information/.

Australian Law Reform Commission, *What is 'personal information'?*, Australian Law Reform Commission, accessed 26 September 2025, https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/6-the-privacy-act-some-important-definitions/what-is-personal-information.

myID, *How to set up myID*, myID, accessed 26 September 2025, https://www.myid.gov.au/how-to-set-up-myid#myid-Identitystrength.

Office of the Australian Information Commissioner, *Interaction between the Digital ID Act and the Privacy Act*, Australia's Digital ID System, accessed 26 September 2025, https://www.digitalidsystem.gov.au/digital-id-accreditation/privacy-materials-for-accredited-entities/interaction-between-the-digital-id-act-and-the-privacy-act.

Office of the Australian Information Commissioner, *Notifiable Data Breaches scheme 12-month insights report*, Office of the Australian Information Commissioner, accessed 26 September 2025, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-scheme-12-month-insights-report.

Office of the Australian Information Commissioner, *Part 4: Notifiable Data Breach (NDB) Scheme*, Office of the Australian Information Commissioner website, accessed 26 September 2025, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme.

Relationship Authorisation Manager, *Set up your Digital ID and identity strength*, Relationship Authorisation Manager, accessed 26 September 2025, https://info.authorisationmanager.gov.au/link-to-a-business-in-ram/set-up-your-digital-id-and-identity-strength.