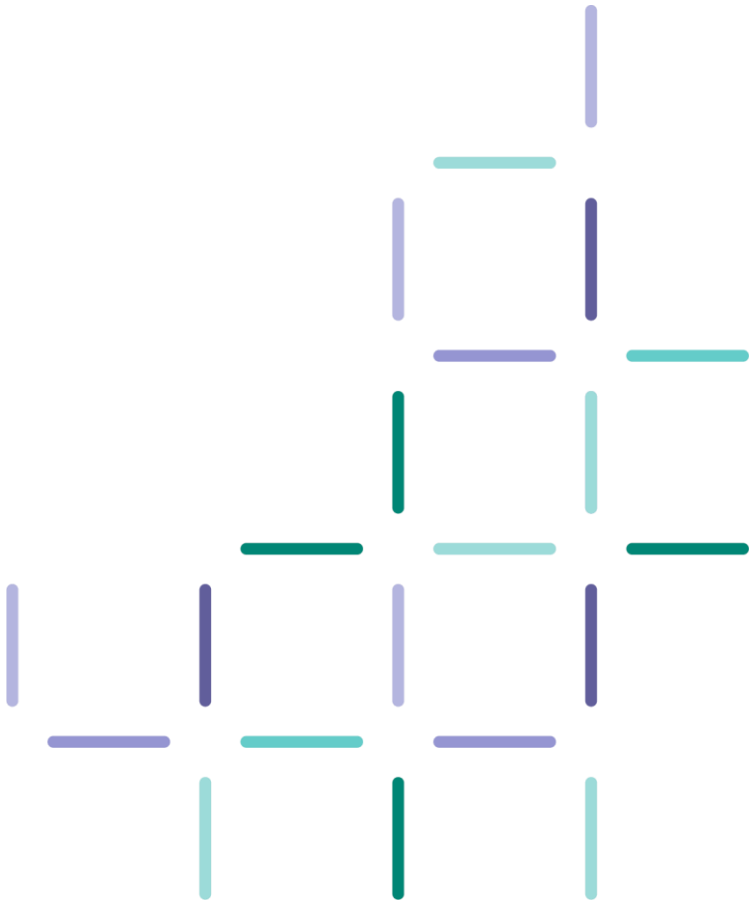
Australian Government

Australia's Digital ID System



Consultation Outcomes 2025 Report: Proposed amendments to the Digital ID Rules and Digital ID (Accreditation) Rules

November 2025

digitalidsystem.gov.au

Department of Finance

Contents

1. Executive summary

Overview

1.1. This Report summarises the outcomes of consultation on proposed amendments to the *Digital ID Rules 2024* (**Digital ID Rules**) and the *Digital ID (Accreditation) Rules 2024* (**Accreditation Rules**), including key changes made to the exposure draft rules to reflect consultation feedback before they were made by the Minister.

1.2. Australia's Digital ID System comprises an Australian Government Digital ID System (**AGDIS**) and an accreditation scheme for digital ID service providers operating within and beyond the AGDIS, both of which operate under the *Digital ID Act 2024* (**Digital ID Act**). The Digital ID Act aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses.

1.3. The Digital ID Act authorises the Minister to make the rules for the AGDIS and the accreditation scheme. The *Digital ID Rules 2024* (**Digital ID Rules**) and the *Digital ID (Accreditation) Rules 2024* (**Accreditation Rules**) commenced at the same time as the Digital ID Act, on 30 November 2024. The Act and Rules establish a robust and effective legal framework governing the AGDIS and the accreditation scheme.

Proposed amendments

1.4. Exposure drafts of proposed rules to amend the Digital ID Rules and the Accreditation Rules were released for public consultation from 18 September to 17 October 2025. The *Digital ID Amendment (Redress Framework and Other Measures) Rules 2025* (**Digital ID Amendment Rules**) and the *Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025* (**Accreditation Amendment Rules**) focus on strengthening consumer protections, enhancing system integrity, and improving operational efficiency.

1.5. The Digital ID Amendment Rules establish a redress framework for individuals affected by cyber security and digital ID fraud incidents that occur in relation to accredited services of accredited entities within the AGDIS. This framework is required under subsection 88(1) of the Digital ID Act and must be provided for in the Digital ID Rules within 12 months of the Act's commencement on 30 November 2024. The Digital ID Amendment Rules also provide for streamlined applications to participate in the AGDIS when made by government entities receiving digital ID services due to machinery of government changes, and authorise the Digital ID Data Standards Chair to use the Digital ID Trustmark.

1.6. The Accreditation Amendment Rules update protective security requirements to the latest release of the Protective Security Policy Framework (**PSPF**), extend the maximum period of consent for business use of a digital ID, and defer the commencement of suspension provisions to allow for technical readiness.

What did we hear?

1.7. The Department of Finance (**Department**) received 51 submissions, approximately half of which provided feedback about the exposure draft rules. The Department also received verbal feedback from a range of parties, including consumer and privacy advocates, inclusion representatives, government agencies, and digital ID service providers.

1.8. Stakeholders broadly supported the objectives of the proposed amendments, particularly measures in the redress framework to support digital ID users affected by cyber security or digital ID fraud incidents. Feedback emphasised the importance of timely notification to individuals affected by incidents, clear and accessible complaints handling processes, and robust oversight of investigations. Privacy advocates highlighted the need for strong safeguards in the redress framework and recommended guidance to ensure consistent application of notification obligations.

1.9. Industry participants welcomed the proposed extension of consent periods for business use of digital ID and streamlined arrangements for machinery of government changes.

1.10. There was general agreement and positive support for aligning the Accreditation Rules with the latest PSPF requirements. Stakeholders viewed the proposed PSPF alignment and the deferral of suspension provisions as practical and sensible steps.

1.11. Minor feedback regarding the PSPF was received regarding the need to clarify some areas of ambiguity, and about limiting the application of PSPF requirements solely to non-corporate Commonwealth entities (**NCEs**). This approach may present challenges for private sector entities that carry out government business and therefore hold government information but are not classified as NCEs.

Changes from feedback

1.12. The Minister considered the relevant issues raised during consultation and in written submissions before making the final rules.

1.13. Feedback on the exposure draft Digital ID Amendment Rules resulted in strengthening the obligation to notify individuals under the redress framework. The revised rules establish a presumption in favour of notifying affected individuals, unless this could cause harm to the individual or have a material effect on the AGDIS. Guidance will be developed by the Digital ID Regulator and the System Administrator in relation to various aspects of the redress framework.

1.14. Feedback on the exposure draft Accreditation Rules resulted in the inclusion of a 12 month transitional period for entities to change from the Protective Security Policy Framework to ISO/IEC 27001 or equivalent options.

Next steps

1.15. The Department will support the Digital ID Regulator to develop guidance materials that support implementation of the redress framework and promote compliance. These

materials are expected to cover notification obligations, referral obligations, and policy publication standards.

1.16. The Government will continue to engage with stakeholders on arrangements for private sector participation in the AGDIS and to progress the necessary rules and standards needed for this phase of the AGDIS.

Conclusion

1.17. The Government thanks stakeholders for actively participating in the consultations, informing the development of the amendment rules.

2. Digital ID legislative framework overview

2.1. This Report summarises the outcomes of consultation on proposed amendments to the *Digital ID Rules 2024* (**Digital ID Rules**) and the *Digital ID (Accreditation) Rules 2024* (**Accreditation Rules**), including key changes made to the exposure draft rules to reflect consultation feedback before they were made by the Minister.

2.2. Australia's Digital ID System comprises an Australian Government Digital ID System (**AGDIS**) and an accreditation scheme for digital ID service providers operating within and beyond the AGDIS, both of which operate under the *Digital ID Act 2024* (**Digital ID Act**). The Digital ID Act aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses.

2.3. The Digital ID Act and the accompanying *Digital ID (Transitional and Consequential Provisions) Act 2024* were passed by the Australian Parliament and received Royal Assent in May 2024.

2.4. The Digital ID Act authorises the Minister to make rules for the AGDIS and the accreditation scheme, including the *Digital ID Rules 2024* (**Digital ID Rules**) and *Digital ID (Accreditation) Rules 2024* (**Accreditation Rules**).

2.5. The Digital ID Act also authorises the Digital ID Data Standards Chair to make the data standards for technical integration requirements for entities to participate in the AGDIS, and technical, data or design standards relating to accreditation (if required to do so by the Accreditation Rules or the Digital ID Rules). The *Digital ID (Accreditation) Data Standards 2024* (**Accreditation Data Standards**) and *Digital ID System Data Standards 2024* (**AGDIS Data Standards**) are together, referred to collectively as the **data standards**.

2.6. Each of the abovementioned rules and data standards were made on 7 November 2024, to commence at the same time as the Digital ID Act on 30 November 2024.

2.7. When the digital ID legislative framework is referred to, the Digital ID Act, the Digital ID Rules, the Accreditation Rules, the Accreditation Data Standards and the AGDIS Data Standards are being referred to.

2.8. The digital ID legislative framework creates:

- the legislated accreditation scheme for digital ID service providers operating within and beyond the AGDIS
- the legislated AGDIS for participating entities
- independent regulatory oversight functions, including a Digital ID Regulator, a System Administrator for the AGDIS and an expanded role for the Information Commissioner
- additional privacy and other safeguards.

2.9. Initially, only public sector entities can participate in the AGDIS. Over time, participation will expand to include private sector organisations who will be able to apply to the

Digital ID Regulator for approval to participate in the AGDIS by no later than two years after the Act commenced.

2.10. Copies of the Digital ID Act, rules and data standards (and their accompanying explanatory materials), can be accessed from the Federal Register of Legislation at: www.legislation.gov.au. Further information about the Digital ID legislative framework can be accessed from the digital ID website at: www.digitalidsystem.gov.au/what-is-digital-id/digital-id-act-2024.

3. Approach to public consultation

3.1. Section 169 of the Digital ID Act generally provides for consultation requirements before making or amending rules under section 168 of the Act. Specifically, the Minister for Finance (**Minister**) is required to publish a notice on the Department's website, setting out the draft rules and inviting submissions for a minimum period of 28 days. The Minister must consult organisations representing individuals who may face barriers in using digital ID services, by written invitation with at least 28 days to respond. All submissions and comments received within the specified periods must be considered.

3.2. The Department upheld consultation requirements under the Digital ID Act as follows.

3.3. Exposure drafts of proposed rules to amend the Digital ID Rules and the Accreditation Rules, their accompanying explanatory statements and materials for public consultation, were published on the Department's website from 18 September 2025 to 17 October 2025.

3.4. Public submissions were invited. Participants could submit comments either through a web-based comment channel or by providing written feedback on the consultation materials and exposure drafts. They could choose to give feedback anonymously and confidentially.

3.5. The Department received 51 submissions, approximately half of which provided feedback about the exposure draft rules. The Department also received other feedback during consultation activities from a range of parties, including consumer and privacy advocates, inclusion representatives, government agencies, and digital ID service providers.

3.6. The consultation process sought to ensure transparency, inclusion and trust. The Department invited organisations representing individuals who may face barriers in using digital ID services to provide verbal or written feedback, and held bilateral meetings with some organisations.

3.7. The Department held consultation sessions including webinars, roundtables and bilateral meetings, engaging with representatives from various sectors such as government agencies, state and territory jurisdictions, inclusion and privacy advocacy groups, accredited entities, AGDIS participating relying parties, industry participants, digital ID professionals, regulatory bodies and individuals. This facilitated broad participation, allowing individuals and organisations from diverse backgrounds and sectors to take part in the consultations.

3.8. Before making the Rules, the Minister considered the relevant issues raised during consultation and in written submissions.

4. Exposure draft rules proposed amendments

Digital ID Amendment Rules

4.1. The exposure draft *Digital ID Amendment (Redress Framework and Other Measures) Rules 2025* (**Digital ID Amendment Rules**) includes the following proposed changes to the Digital ID Rules:

1) A redress framework for individuals affected by cyber security and digital ID fraud incidents that occur in relation to accredited services of accredited entities within the AGDIS. This framework is required under subsection 88(1) of the Digital ID Act, and must be provided for in the Digital ID Rules within 12 months of the Act's commencement on 30 November 2024. The redress framework contains the following features:
    - Attribute Service Providers (**ASP**) and Identity Services Providers (**ISP**) are required to make reasonable attempts to notify individuals affected by cyber security and digital ID fraud incidents
    - ASPs and ISPs are required to publish cyber security and digital ID fraud incident management policies
    - ASPs and ISPs are required to publish complaints handling policies
    - ASPs and ISPs are required to refer unresolved technical issues to the System Administrator within 28 days and empowering the System Administrator to make recommendations.
2) The System Administrator is empowered to direct investigations into cyber incidents and digital ID fraud incidents.
3) The Digital ID Data Standards Chair is authorised to use the digital ID trustmark.
4) A streamlined application for participation in the AGDIS is provided for government relying parties receiving services due to a machinery of government change.

Accreditation Amendment Rules

4.2. The exposure draft *Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025* (**Accreditation Amendment Rules**) contained the following proposed changes to the Accreditation Rules:

1) Updating protective security requirements to the latest release of the Protective Security Framework (**PSPF**) and limiting its application to non-corporate Commonwealth entities (**NCEs**), with other entities to use an alternative protective security framework.

2) Introducing a 7 year maximum expiry period for express consent given to an ASP by individuals acting for or on behalf of a business, while retaining the 12 month maximum period of consent for personal use.

3) Deferring by 12 months obligations on transitioned accredited entities to suspend and resume an individual's digital ID at their request, in response to feedback that complying with these requirements have proven to be operationally and technically challenging.

5. Feedback themes and post-consultation revisions

Overall summary

5.1. Stakeholders broadly welcomed the proposed amendments to the Digital ID Rules and Accreditation Rules, recognising their importance in supporting affected individuals, providing clearer pathways for managing incidents within the AGDIS, improving transparency and strengthening governance.

5.2. Overall, submissions made about both exposure draft rules agreed that the amendments represent a positive step toward a more secure, transparent, and inclusive Digital ID System. However, they emphasised the need for clear guidance and a strong commitment to accessibility and consumer protection.

Digital ID Amendment Rules

5.3. A recurring theme in submissions was emphasis on the need for practical guidance for both digital ID service providers and individuals about how the redress framework and other amendments should be implemented and how they would apply in different scenarios. Stakeholders recommended that the System Administrator and Digital ID Regulator should publish guidance to support consistent implementation, promote compliance, and build public confidence.

5.4. Consumer and civil society groups called for stronger obligations to notify individuals affected by cyber security or digital ID fraud incidents, stressing timely and accessible communication to enable protective action. Industry supported user support pathways and enhanced investigative powers but emphasised proportionate obligations and practical timeframes.

5.5. Views diverged regarding the proposed 28 day timeframe for referring unresolved issues to the System Administrator. Industry considered this reasonable, while consumer advocates argued for shorter timeframes.

5.6. Stakeholders broadly supported publishing incident management and complaints policies to promote transparency, recommending clear, accessible formats and translations. Some cautioned against technical detail that could expose vulnerabilities, while ensuring individuals understand the steps to be taken.

5.7. The following table summarises the feedback received in relation to specific aspects of the exposure draft of the Digital ID Amendment Rules, and sets out the where the rules have been revised in response to feedback.

Measure	Feedback summary	Revision or response
Redress – notifying individuals: The exposure draft rules established an obligation for ISPs and ASPs to *consider notifying* individuals affected by cyber security or digital ID fraud incidents, taking into account the likelihood of harm to individuals and material effect on the AGDIS.	Submissions strongly and consistently supported notifying affected individuals. Many recommended strengthening the notification obligation rather than leaving it to the entity's discretion; some raised concern with the apparent equal weighting of harm to individuals and system impact; some suggested aligning with the Mandatory Notifiable Data Breach scheme under the *Privacy Act 1988* (**Privacy Act**).	The Digital ID Amendment Rules were revised to strengthen the obligation to notify - to a presumption in favour of notification, unless notification could result in harm to the individual or have a material effect on the AGDIS. Guidance will be developed to support implementation. Privacy Act obligations also apply to incidents that meet the threshold under that Act.
Redress – entity scope: Redress framework obligations are limited to ISPs and ASPs only.	A few submissions recommended extending the redress obligations to identity exchanges and/or relying parties, or noted that there was no clear coordination of responsibility for entities not within scope of the redress framework.	The redress framework is limited to ISPs and ASPs as they are best positioned to support consumers and manage incidents that arise in relation to accredited services in the AGDIS. Relying parties and exchanges are subject to preexisting obligations in the Digital ID Rules to notify the System Administrator of all cyber security and digital ID fraud incidents. Exchanges do not interact with individuals and do not have public-facing services; they only interact with other entities. Relying parties are the consumers of accredited services, and incidents within their control will most likely relate to their own non-AGDIS services. Guidance will be developed to support implementation.

Measure	Feedback summary	Revision or response
Redress – incident scope: Redress framework obligations are limited to cyber security and digital ID fraud incidents.	A small number of submissions recommended expanding obligations beyond cyber security and digital ID fraud incidents to include technical issues, outages, and accessibility problems.	The redress incident response obligations deliberately align with and build on the existing cyber security and digital ID fraud incident notification obligations in the Digital ID Rules. The rules impose strict incident notification obligations on these types of incidents, and the System Administrator has a specific function under the Act to manage these incidents.
Redress – notification timeframes: The notification provisions do not include additional timeframes.	A small number of submissions recommended introducing a maximum timeframe for determining whether to notify individuals.	The existing obligation on participating entities to notify the System Administrator within one (1) business day of all cyber security or digital ID fraud incidents, includes a requirement to explain when individuals were informed of the incident, or why the individual has not been informed. This existing provision ensures there is a timeframe within which entities must have assessed whether to notify individuals, and provides a mechanism by which the System Administrator will be aware as to whether individuals have been notified.

Measure	Feedback summary	Revision or response
Redress – publishing complaints and incident management policies: The exposure draft rules require ISPs and ASPs to publish policies on: 1. Complaints, including how to make a complaint, contact details, complaints procedures, and timeframes; and 2. Cyber security and digital ID fraud incident management.	Most submissions welcomed these obligations, noting this would improve transparency and user confidence. Several submissions cautioned against over-disclosure of sensitive details that could benefit threat actors and/or compromise security. Several submissions recommended called for minimum standards, plain language, and accessibility (including multilingual and offline formats). Some recommended guidance on scope, interaction with existing obligations, and security sensitivities. Some recommended a longer transition period to facilitate compliance.	The exposure draft rules have been amended to provide that entities have until 1 July 2026 to comply with the publication obligation (approximately one (1) additional month). Accredited entities are subject to existing usability and accessibility obligations under the Accreditation Rules, including requirements for usability testing, Web Content Accessibility Guidelines (WCAG) compliance, plain language, multiple accessible formats, and processes for user assistance and complaints. Guidance will be developed to support implementation.
Redress – referral of unresolved issues to System Administrator: The exposure draft rules require ISPs and ASPs to refer unresolved technical issues to the System Administrator within 28 days.	Submissions broadly supported referring unresolved technical issues to the System Administrator, one submission opposed referral. Views varied on the 28 day timeframe, several suggested shorter periods for critical issues while some supported 28 days. Some recommended there be less discretion for deciding whether issues and mandatory referral for unresolved complaints. Some submissions recommend that entities should also be required to report on trends in complaints and /or technical issues.	The discretion to determine whether technical issues can be resolved is retained, reflecting operational realities and avoiding referral of low risk matters to the System Administrator. The 28 day period is retained to enable sufficient time for complex issues, though entities may refer matters in a shorter period. Guidance will be developed to support implementation. Accredited entities are currently subject to record-keeping and incident reporting, but not annual reporting. Reporting on technical issues and complaints should be considered as part of the statutory review into the operation of the Act.

Measure	Feedback summary	Revision or response
Redress – System Administrator recommendation power: The exposure draft rules empower the System Administrator to recommend a course of action for unresolved issues.	Some submissions suggested that the System Administrator's power to recommend a course of action should be strengthened to enhance accountability.	The recommendation power is calibrated to the System Administrator's function to coordinate, support, and maintain the performance and integrity of the AGDIS and with its existing powers under the Act. The System Administrator has existing powers under section 130 of the Digital ID Act to issue binding directions to entities to protect the integrity or performance of the system, with civil penalties for non-compliance. The recommendation power therefore serves as a proportionate operational tool for the System Administrator to promote improvements and coordination, while retaining the capacity to use its directions power if appropriate.
Reportable incident investigations: The exposure draft rules empower the System Administrator to direct any entity that interacted with the affected digital ID to investigate. The entity must start promptly, provide findings when complete, and give updates every 28 days if delayed.	There was broad support for strengthening oversight and giving the System Administrator authority to direct investigations; one (1) submission did not support. Many submissions raised practical concerns about implementation, particularly around the 28 day period and clarity of expectations. Some suggested guidance on the purpose, scope and circumstances of investigations to reduce uncertainty.	Investigations are intended to determine whether a digital ID has been compromised or misused and to assess any potential impact on other entities that have interacted with that ID. The 28 day period is retained to enable sufficient time for complex issues, though entities may provide updates in a shorter period where possible. Guidance will be developed to support implementation.
Trustmark authorisation: Authorising the Digital ID Data Standards Chair to use the trustmark	Stakeholders all supported this amendment.	No change to the amendment rules.

Measure	Feedback summary	Revision or response
Machinery of government changes: Streamlining applications for government relying parties receiving a previously approved service due to a machinery of government change	Feedback was broadly positive, noting this could reduce delays. A small number of submissions highlighted the importance of maintaining privacy obligations across the transition between the transferring and receiving entities.	No change to the amendment rules.

Accreditation Amendment Rules

5.8. Submissions broadly supported the intention of the proposed amendments.

5.9. Submissions broadly supported a longer duration of express consent for business purposes. Some privacy and advocacy organisations suggested a shorter period and/or additional reminders. Industry and business groups supported the proposed seven (7) year period to reduce administrative burden.

5.10. There was broad agreement on aligning protective security requirements with the PSPF for certain entities. Some feedback noted challenges for private sector entities holding government information but not classified as non-corporate Commonwealth entities (NCEs), and sought clarification on areas of ambiguity.

5.11. The following table summarises the feedback received in relation to specific aspects of the exposure draft of the Accreditation Amendment Rules, and sets out the where the rules have been revised in response to feedback.

Measure	Feedback summary	Revision or response
Protective Security Policy Framework (PSPF): Updating compliance requirements for the PSPF, mandating its use for non-corporate Commonwealth entities; ISO/IEC 27001 or equivalent remains an option for others.	Generally, all submissions received were supportive of this change to reflect the latest versions of the PSPF. A few stakeholders raised concerns that a longer transition period will need to be provided to assist non-NCEs currently adopting the PSPF and to clarify some ambiguity in rule 4.2.	Amendment rules revised to provide a transitional period provided for non-NCE's with a further 12 months to transition from the PSPF to the ISO/IEC 27001 requirements or an alternative framework under rule 4.2(1). The language in rule 4.2 was clarified to delineate clearly the respective duties of non-NCE's and NCEs. Rules otherwise not changed.
Consent expiry period: Introducing a separate 7 year maximum expiry	Broadly all submissions supported a separate consent period for business use.	No change to the amendment rules.

Measure	Feedback summary	Revision or response
period for express consent given to an ASP by individuals acting for or on behalf of a business, while retaining the 12 month maximum period of consent for personal use.	Most submissions supported the proposed 7 year period. A small number of stakeholders suggested a shorter period would be appropriate. Several recommended safeguards, such as periodic reminders to maintain informed consent.	
Suspension and resumption obligations: Deferring digital ID suspension and resumption obligations for transitioned accredited entities until 30 November 2026, to allow technical readiness.	Deferral of obligations was broadly supported, acknowledging that these mechanisms should not be removed.	No change to the amendment rules.

6. Next steps

6.1. Consultation feedback emphasised the need for clear guidance for entities and individuals on how the rules will work in practice. The Department will support the Digital ID Regulator to develop guidance materials that support implementation of the redress framework, promote compliance and build public confidence. These materials are expected to cover notification obligations, referral obligations, and policy publication standards.

6.2. From 30 November 2026, the Digital ID Act will enable private sector relying parties and accredited entities to apply to the Digital ID Regulator for approval to participate in the Australian Government Digital ID System (subsection 61(d) of the Digital ID Act). The Government is preparing operational changes needed for private sector entities to participate. The Government will continue to engage with stakeholders on proposed arrangements and intends to progress necessary rules and standards required to support private sector participation should the Digital ID Regulator approve entities to participate.

6.3. The Digital ID Data Standards Chair is appointed under the Digital ID Act to make Digital ID Data Standards. It is expected the Chair will make (or amend) any data standards that are required to enable private sector participation in the AGDIS.

6.4. A statutory review into the operation of the Digital ID Act will be undertaken within two years of the commencement of the Act (i.e., by 30 November 2026), as required by section 162 Digital ID Act.

7. Conclusion

7.1. The Government thanks stakeholders for actively participating in the consultations, informing the development of the amendment rules.