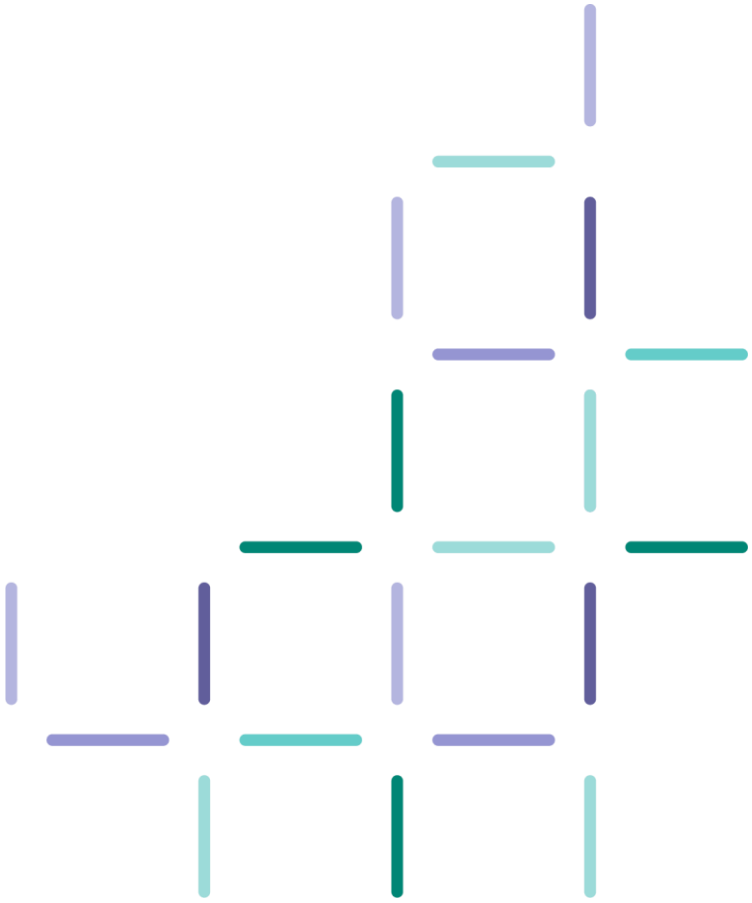
Australian Government

Australia's Digital ID System



November 2024

Digital ID Subordinate Legislation Consultation Outcomes

digitalidsystem.gov.au

Table of contents

Executive summary

Australia's Digital ID System comprises an accreditation scheme for digital ID service providers and an Australian Government Digital ID System (AGDIS) both of which, from 1 December 2024, will operate under the *Digital ID Act 2024* (**the 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. The Act is supported by a range of rules and data standards that set out additional details of the accreditation scheme and AGDIS.

The Digital ID Act authorises the Minister to make the rules for the Digital ID accreditation scheme and AGDIS: the *Digital ID Rules 2024* (the **Digital ID Rules** and *Digital ID (Accreditation) Rules 2024* (the **Accreditation Rules**). The Digital ID Act also authorises the Digital ID Data Standards Chair (initially the Minister) to make the data standards for the Digital ID accreditation scheme and the AGDIS: *Digital ID (Accreditation) Data Standards 2024* (the **Accreditation Data Standards**) and *Australian Government Digital ID System Data Standards 2024* (the **AGDIS Data Standards**).

These are collectively called the **rules and data standards**. They establish a robust and effective legal framework governing the accreditation scheme and AGDIS. Promoting trust in digital ID services, by ensuring less data is shared and stored, and in a more secure way, will also facilitate economic benefits for, and reduce burdens on, the Australian economy.

Exposure drafts of the rules and data standards were released for public consultation in mid-2024. This report summarises the outcomes of these consultations, including key changes made to the exposure draft rules and data standards to reflect consultation feedback before they were made by the Minister.

What did we hear?

Most stakeholders supported the general objectives and purpose of the rules and data standards, particularly privacy safeguards and other rules designed to promote the accessibility and usability of Digital ID services.

They also provided views on amendments and broader regulatory implementation suggestions such as the importance of:

- appropriate guidance for accredited entities and entities participating in the AGDIS on their responsibilities under the rules and data standards,

- ongoing communication and targeted consultations to promote trust in the regulatory framework,
- enhancing inclusion, consumer experience, and consumer support for adoption of Digital ID,
- promoting privacy, security, and fraud control by ensuring these requirements adapt to emerging risks and technological advancements, and
- careful management and coordination of incident responses as the AGDIS and the accreditation scheme expands by aligning incident reporting with other national data breach frameworks to facilitate 'one-stop reporting' and reduce redundant regulatory requirements.

The private sector strongly advocated accelerating their participation in AGDIS, by allowing them to join sooner than the maximum timeframe allowed under the Digital ID Act (being 2 years from the commencement of the Digital ID Act in December 2024).

Stakeholders who strongly opposed the rules and data standards overall also firmly opposed the Digital ID Act.

Changes from feedback

Feedback on the Accreditation Rules resulted in amendments to further clarify requirements including record-keeping, reportable incident requirements, data minimisation obligations, and requirements on the duration of a user's express consent. Additionally, arrangements have been provided in the Accreditation Rules for entities transitioning their accreditation from the Trusted Digital Identity Framework (TDIF) pilot accreditation program to the legislated accreditation scheme.

The draft Digital ID Rules and Accreditation Rules included conditions that would have made it easier for entities who have reporting obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the AML/CTF Act) to use an accredited identity service provider (ISP) to collect a limited set of restricted attributes such as ID document numbers, for the purposes of complying with their AML/CTF obligations. These conditions have been removed, based on consultation feedback that other options for meeting AML/CTF obligations should be explored, to examine whether there are ways that involve less reliance upon the sharing of restricted attributes.

To reduce unnecessary duplication of regulatory obligations the Digital ID Rules now relies on the Accreditation Rules for contractor requirements and aligns its record keeping period to 3 years (reduced from 6 years) for consistency with the Accreditation Rules.

Feedback on the Digital ID Rules resulted in amendments to allow the System Administrator, Information Commissioner, Digital ID Regulator and the Secretary of the Department to use or display the Digital ID Accreditation Trustmark in certain

circumstances such as education about the Digital ID Act. Other changes included minor clarifications about cyber security and digital ID fraud incident reporting timeframes and mandatory reporting circumstances; and the transition of limited-liability arrangements for government entities on an interim basis (addressed in the Transitional Rules). Feedback on the AGDIS Data Standards led to several technical amendments and clarifications, and removal of unnecessary requirements or requirements that would have had unintended impacts.

The AGDIS Data Standards enable the AGDIS to shift from a ‘double blind’ to a ‘single blind’ approach. Under a single blind approach, the Identity Exchange would continue to conceal from identity service providers which relying party services users are accessing with their Digital ID.

Feedback was received on the Identity Exchange’s use of a ‘single blind’ instead of a ‘double blind’ IT-based privacy solution. The single blind approach aligns with legislated privacy safeguards to prohibit data profiling (mitigating the need for such an IT solution), and allows for enhancing user experience, fraud detection, and increased private sector AGDIS participation by entities with AML/CTF reporting obligations. Additionally, it requires the Identity Exchange to uphold assurance and transparency through annual published audits of the information provided to relying parties.

Next steps

The Government will continue to progress the necessary rules and standards needed for the further expansion of Australia’s Digital ID System.

The Government will collaborate with the Data Standards Chair (appointed under the Digital ID Act), to ensure the rules align with the data standards as required.

Background

Digital ID legislative framework

The *Digital ID Act 2024* (**Digital ID Act**) is the primary legislation for the accreditation scheme and the AGDIS. The Digital ID Act and the related *Digital ID (Transitional and Consequential Provisions) Act 2024* (**Transitional Act**) were passed by the Australian Parliament and received Royal Assent in May 2024. This legislation authorises multiple legislative instruments which govern the Digital ID accreditation scheme and AGDIS.

Specifically, the Digital ID Act authorises the Minister to make the rules for the Digital ID accreditation scheme and AGDIS: the *Digital ID Rules 2024* (the **Digital ID Rules)** and *Digital ID (Accreditation) Rules 2024* (the **Accreditation Rules**). The Digital ID Act also authorises the Digital ID Data Standards Chair (initially the Minister) to make the data standards for the Digital ID accreditation scheme and the AGDIS: *Digital ID (Accreditation) Data Standards 2024* (the **Accreditation Data Standards**) and *Australian Government Digital ID System* Data Standards 2024 (the **AGDIS Data Standards**).

The Digital ID Act further authorises the Minister to make the *Digital ID (Phasing-in of Participation in the Australian Government Digital ID System) Determination 2024* (the **Phasing Determination**). The Phasing Determination enables State and Territory entities to apply to the Digital ID Regulator for approval to participate in AGDIS from commencement of the Digital ID Act, as both relying parties and accredited entities (although no states and territories have sought accreditation at this stage).

The related Transitional Act enables the Minister to make the *Digital ID (Transitional and Consequential Provisions) Rules 2024* (the **Transitional Rules**). The Transitional Act and Transitional Rules deal with consequential and transitional matters arising from enactment of the Digital ID Act.

Each of the abovementioned rules, data standards and Phasing Determination were made on 7 November 2024, to commence at the same time as the Digital ID Act on 1 December 2024.

A schematic of the legislative framework (excluding those instruments dealing with transitional matters) is shown in Figure 1. In summary, the framework creates:

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

On commencement of the Digital ID Act, any provider of digital ID services (including government and private sector entities) may apply for accreditation under the legislated accreditation scheme as set out in the Accreditation Rules and Accreditation Data Standards. Accreditation is voluntary, meaning that only entities that apply to be accredited will be subject to the obligations in the accreditation scheme.

Initially, only public sector entities can participate in the AGDIS under the Digital ID Rules and AGDIS Data Standards. 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 by no later than two years after the Act commences (i.e. December 2026).

Copies of the rules and data standards and the Explanatory Statements, which explain the content and purpose of each legal instrument, 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 website at: www.digitalidsystem.gov.au/what-is-digital-id/digital-id-act-2024

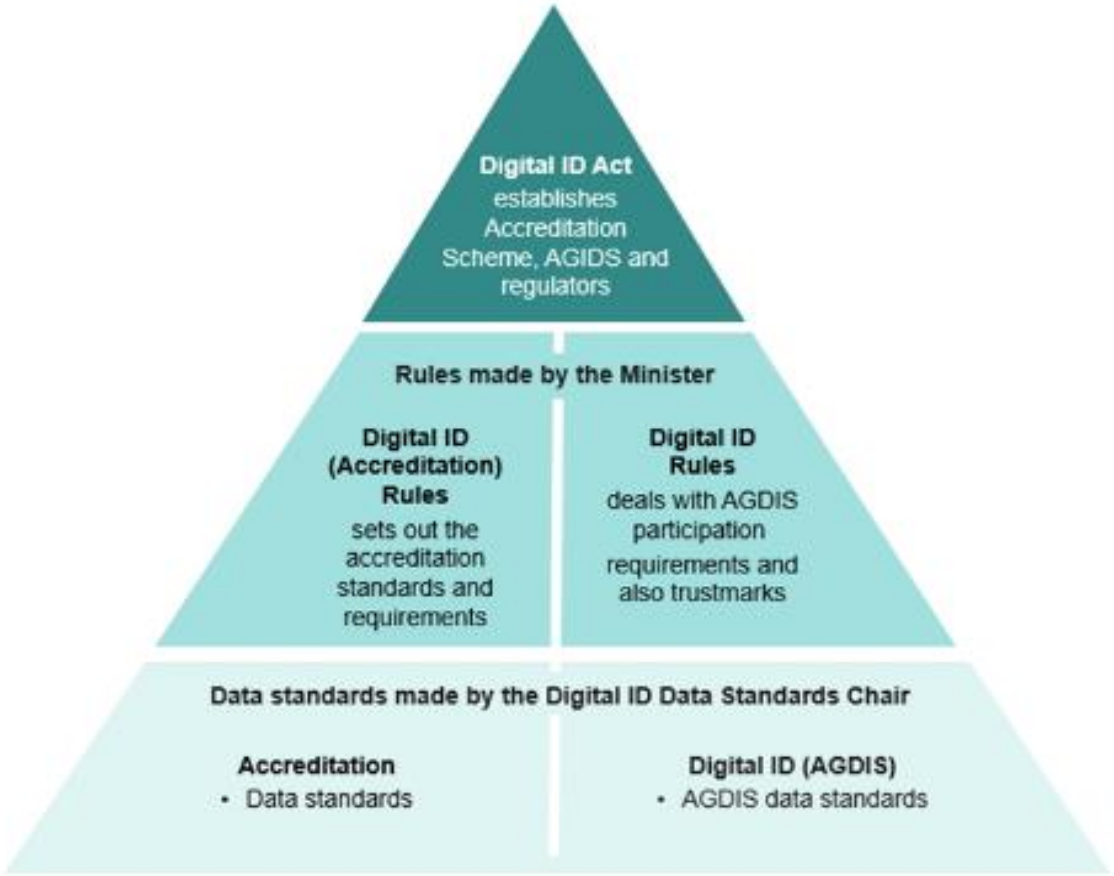


Figure 1: Digital ID legislative framework

Approach to public consultation

The rules and data standards have been informed by feedback from previous consultations, including the 2023 consultation on the Digital ID legislation (the Digital ID Bill 2023, Digital ID Rules and Accreditation Rules), as well as several years of consultation on the TDIF – the policy framework that preceded the legislation – including through the TDIF pilot accreditation program.

The 2024 consultations aimed to gather insights and feedback to inform the making of the rules and data standards. The key focus of the consultations was on changes made since previous consultation drafts were released for public comment in September 2023.

The consultation process sought to ensure transparency, inclusion, and trust while supporting the phased development of the digital ID framework. It also built on 6 years of community and industry consultations under the TDIF, and feedback received on draft Accreditation Rules and Digital ID Rules between September and October 2023. Throughout, this effort involved ongoing engagement with government agencies, state jurisdictions, and regulatory bodies.

Method

From 28 May 2024 to 25 June 2024 (28 days), the Government released exposure drafts of the Digital ID Rules, Accreditation Rules, and the Accreditation Data Standards with accompanying materials for public consultation. More than 250 organisations including government bodies, private sector, advocacy groups, and industry representatives engaged in these consultations. Additionally, the Government consulted with 28 inclusion stakeholder groups representing various advocacy and consumer organisations.

From 8 July 2024 to 12 August 2024 (35 days), the Government released an exposure draft with accompanying material for public consultation on the AGDIS Data Standards. In total 16 organisations, including private sector organisations, government agencies, and individuals, participated in these consultations.

Overall, for the 2024 consultations the Government held over 30 consultation sessions including webinars, roundtables and bilateral meetings, engaging with representatives from over 250 organisations from various sectors such as government, private sector, inclusion and privacy advocacy groups, accredited entities, AGDIS relying parties, state and territory jurisdictions, industry participants, digital ID professionals and individuals. This facilitated broad participation, allowing individuals and organisations from diverse backgrounds and sectors to take part in the consultations.

In addition to a call for public submissions, stakeholders were also invited to participate in a consultation session if they had previously submitted feedback on the Digital ID legislative framework (including the Digital ID Bill and its earlier rule drafts), were

engaged or interested in Digital ID matters, or had reached out to the Government during the consultation period to request a meeting.

The Government invited feedback through consultations papers with questions and exposure drafts of the rules and data standards, as published on the Department's website. 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.

Consultations on the Digital ID Rules, Accreditation Rules and Accreditation Data Standards over a 28-day consultation period in May-June 2024 included:

- 3 webinars.
- 14 roundtables.
- 12 bilateral meetings, and
- receiving 42 detailed submissions and 27 webform comments.

Consultations on the AGDIS Data Standards over a 35-day consultation period in July-August 2024 included feedback from many sources including individuals, private organisations and government entities; with 16 submissions received. It also included bilateral meetings with stakeholders to clarify feedback and further refine the AGDIS Data Standards.

Key consultation themes

During the 2024 consultations, stakeholders generally expressed positive feedback and support for the rules and data standards. However, they emphasised the necessity of ongoing consultations, particularly regarding complex policy areas with potential economy-wide implications. They emphasised the importance of:

- ongoing involvement to develop rules and data standards for AGDIS expansion that effectively address key issues for individuals and businesses, and
- additional support for understanding the legislative structure designed for different stakeholder groups, and communication materials that emphasise the benefits of Digital ID.

Key factors identified by stakeholders for promoting the adoption of digital ID included voluntariness, ease-of-use, inclusivity, trust in the accreditation scheme and AGDIS, data privacy and protection, and availability of guidance and support for individuals (including redress arrangements).

Industry stakeholders requested educational resources to help meet regulatory compliance and mandatory reporting requirements. This included encouraging the Government to seek opportunities to:

- streamline where possible the mandatory reporting obligations in the rules and data standards rather than duplicate other national regulatory schemes e.g. *Privacy Act 1988* (the Privacy Act), Security *of Critical Infrastructure Act 2018* (the SOCI Act*)*,
- expedite private sector participation in the AGDIS; implement statutory contract, charging, warranty, liability and redress rules as well as interoperability arrangements among AGDIS participants, and
- achieve alignment and consensus among stakeholders on matters like data localisation, AGDIS service level agreements, international accords, corporations' obligations, additional digital ID trustmark options, and innovations promoting inclusion and trust building initiatives.

Inclusion advocates strongly advised that all individuals, regardless of their background or demographics, should have equitable access to digital ID opportunities and services and that digital ID service providers and relying parties prioritise digital ID inclusion and eliminate any barriers that prevent participation.

There was an overall call for plain language guidance for digital ID service providers and individuals about the scope of the rules and data standards and how they apply in different scenarios, in particular:

- better explanations of where digital ID systems fall within the legislative scheme, and when they might operate outside of it (especially in cases where a service has both accredited and unaccredited components),
- guidance on voluntariness and consent, and
- notification and reporting obligations and coordination with the Notifiable Data Breach Scheme under the Privacy Act.

Following the 2024 consultation on the exposure drafts of the rules and data standards, the Government made changes to ensure the instruments were ready to support the commencement of the Digital ID Act on 1 December 2024.

The consultation emphasised the importance of guidance for consumers and businesses on how the rules and data standards will work in practice. Accordingly, the Office of the Australian Information Commissioner (OAIC, Information Commissioner), System Administrator, and the Digital ID Regulator have prepared guidance materials for commencement of these regulatory arrangements.

Stakeholder feedback will also inform any future updates to rules and data standards that are needed to support private sector participation in the AGDIS.

Digital ID Rules

The key changes to the Digital ID rules resulting from the 2024 consultation are:

- aligning the record keeping time-periods for digital ID prescribed records to the Accreditation Rules (reducing minimum retention timeframes from 6 years to 3 years for prescribed records to balance the need for records to exist to support regulatory action with the need to reduce risks caused by data retention).
- changing the information required to be reported to the System Administrator under the incident reporting framework (to align more closely with current practices in the unlegislated AGDIS).
- leveraging the existing reportable incident rules in the Accreditation Rules for the notification of change in contractors.
- removal of conditions that would have allowed participating relying parties who are reporting entities under the AML/CTF Act to use an accredited ISP to collect a limited set of restricted attributes such as passport numbers, for the purposes of complying with their AML/CTF obligations.
- allowing the Secretary of the Department, the Information Commissioner, Digital ID Regulator and Systems Administrator to use or display the digital ID trustmark (also now known as the Digital ID Accreditation Trustmark) in certain circumstances such as for educational and promotional purposes.

Some proposed rules were removed, on an interim basis, while AGDIS remains 'government only' but will be reassessed for inclusion ahead of 'phasing in' private sector participation, including rules relating to:

- obligations on relying parties participating in the AGDIS to report changes in control, and
- establishment of a statutory contract and requirements in relation to intellectual property rights between entities participating in the AGDIS (for the purposes of subsection 85(1) of the Digital ID Act).

AGDIS Data Standards

The key changes to the AGDIS Data Standards from the consultation are:

- clarification and technical corrections for a number of draft requirements,
- clarification of arrangements for entities using legacy technology, by providing for certain entities to continue using protocols based on Security Assurance Markup Language (SAML) instead of the Open ID Connect protocol.

Single blind

While not a change from the exposure draft, the AGDIS Data Standards allow for the Identity Exchange operated by Services Australia to implement a 'single blind'. The intent

is to enable greater adoption of digital ID and the ability for organisations relying on Digital IDs to meet AML/CTF requirements, while continuing to support strong privacy safeguards.

'Blinding' requirements only apply to identity exchanges participating in the AGDIS. Accredited identity exchanges operating outside of the AGDIS are not required to apply either a single or a double blind. These exchanges may operate different IT architectures that may prevent them from operating a single or double blind, such as a technical register model. However, these exchanges are required to comply with the enhanced privacy safeguards in the Digital ID Act and Accreditation Rules that prohibit the tracking or profiling of individuals accessing services within the digital ID system in which the exchange operates.

Services Australia operates the only exchange in AGDIS which has a double blind approach due to its specific IT architecture. Under the 'double blind' approach in place in AGDIS, the Identity Exchange that brokers information throughout the AGDIS limits the sharing of information in two ways.

- The Identity Exchange does not disclose to an ISP the relying party services that each user accessed with their digital ID, and
- The Identity Exchange does not disclose to relying parties which ISP was used to access their service. Until additional identity service providers join the AGDIS, relying parties will have been aware that users could only have used myID.

The double blind was established in the context of the TDIF pilot accreditation program. This created a technical barrier to the tracking and profiling of user behaviour across the system, in the absence of legislated privacy safeguards and civil penalties for non-compliance. A single blind approach retains the 'side' of the double blind with the most significant benefits for privacy, by continuing to conceal from identity service providers which relying party services individuals are accessing with their digital IDs.

The anticipated benefits of moving to a single blind approach include:

- improved user experience, such as enabling relying parties to reduce the number of screens users must navigate when logging in to access a service,
- stronger fraud detection, as relying parties would have access to additional information that can be used to better detect fraud in a fast-evolving environment,
- better enabling private sector use cases, particularly by small businesses (for example, stakeholders with AML/CTF obligations have cited the double blind as a barrier that would prevent them from joining the AGDIS).

If the Identity Exchange continues to implement a double blind, there is a risk that fewer businesses will participate in the AGDIS and will opt instead to continue scanning and storing copies of identity documents, or operate outside of the system, undermining

the purpose of Digital ID to safeguard personal information by not oversharing details with services or businesses.

Single blind consultation feedback

As well as seeking formal written submissions on this issue, the Government engaged extensively with privacy and human rights stakeholders. An updated Privacy Impact Assessment (PIA) for the Digital ID framework also considered the proposed change.[1]

Overall, stakeholders generally agreed that moving to a single blind approach has potential benefits such as enhancing user experience and boosting business participation, but noted that the change in policy may impact public perception of the privacy protections offered by Digital ID. Some stakeholders suggested that this risk could be mitigated by introducing additional assurance and transparency requirements for the Identity Exchange.

This feedback has informed the introduction of a requirement for the Services Australia Identity Exchange to arrange for regular independent audits of the single blind function, if a single blind is implemented. The audit results must be published. This is a condition of the Identity Exchange's participation in the AGDIS and is set out in the Transitional Rules. The intent is to increase transparency and support the public's continued confidence in the privacy safeguards offered by the AGDIS.

Accreditation Rules and Accreditation Data Standards

The key changes to the Accreditation Rules and Data Standards from the 2024 consultation are:

- clarifying the record keeping timeframes for accredited entities in respect of cyber security and digital ID fraud incidents as well as aligning these with the Digital ID Rules (3-year timeframe within both the Digital ID Rules and the Accreditation Rules).
- removing certain documents such as rates notices and electricity bills from the list of documents and credentials that could be used to create a digital ID, as stakeholders indicated they were difficult to verify and presented fraud risks.
- general clarifications to rules and removal of requirements to reduce regulatory burden, such as clarifications to requirements for the provision of advice to individuals and removal of the journey map requirement.

[1] A copy of the PIA can be accessed from the website at: www.digitalidsystem.gov.au/what-is-digital-id/privacy-and-security

- clarifications around the data retention period of personal information for providers of one-off digital IDs so that ISPs can retain personal information for up to 30 days to enable fraud control processes.
    - After this period, the ISP must destroy that personal information unless it is required by law to retain it.
- removal of conditions similar to those in the Digital ID Rules that would have allowed an ISP to disclose a limited set of restricted attributes for the purposes of allowing relying parties who are also AML/CTF reporting entities to comply with their AML/CTF obligations.
    - The removal of the condition was based on feedback that alternate AML/CTF compliance methods should be explored to reduce reliance on restricted attribute sharing.
- addition of transitional provisions for entities transferring their accreditation from the TDIF pilot accreditation program to the accreditation scheme (referred to in the Accreditation Rules as transitioned accredited entities).
    - These rules delay the application of certain new or changed rules, that they were not previously subject to in the TDIF, for 12 months to give transitioned accredited entities the time necessary to comply with those rules, such as to complete system upgrades.

Next Steps

The Digital ID Act allows a phased AGDIS expansion to include private sector participants no later than 2 years from Act commencement (refer to subsection 61(d) of the Digital ID Act).

Stakeholders provided views on a range of topics relevant to future private sector participation – namely redress and liability, interoperability, charging, and the holding of data outside of Australia – which are summarised in the following section.

These views will be considered as part of developing future policy and rules to enable the private sector to participate in the AGDIS by 1 December 2026.

Some stakeholders noted that the complexity and cost of accreditation posed barriers to some digital ID providers joining the accreditation scheme. The Government recognises these issues and acknowledges the need for ongoing reviews of the Accreditation Rules and Data Standards. Consultations over time have simplified requirements in the Accreditation Rules compared to TDIF, though new requirements were added due to changes in technology and developments in the risk landscape since early 2022.

The Government will keep working with digital ID stakeholders and the Digital ID Regulator to find opportunities to simplify processes for accreditation, leverage existing

regulatory schemes; including maintaining rules and identifying proofing options and fraud mitigation strategies – which are summarised in the following section.

Redress and liability framework – *particularly in respect of handling user complaints and providing redress for issues related to use of Digital IDs in the AGDIS*

Stakeholders emphasised the importance of providing strong support mechanisms for individuals, such as through access to telephone assistance and non-financial redress arrangements, when using digital IDs in the AGDIS. This particularly included support when people are affected by a fraud or cyber incident, or when people need help to create, manage or use a Digital ID with services in the system.

The Digital ID Act includes requirements to make rules on redress arrangements in the AGDIS by 1 December 2025 and provides direction on what the redress framework must and may include. This includes that the rules must specify the entities and kinds of incidents covered by the framework, the procedures for dealing with incidents and providing support, and notification and information provision requirements.

Any future redress rules will build on the Accreditation Rules which currently contain obligations on accredited entities to support individuals affected by a digital ID fraud incident or a cyber security incident; and provisions giving users more control by ensuring they can temporarily suspend a digital ID from use. Additionally, the Digital ID Act supports users' control of digital IDs and requires accredited entities to deactivate a digital ID on request of an individual.

Interoperability – *setting out when entities participating in the AGDIS must interoperate with each other*

Several stakeholders highlighted that interoperability will become increasingly important as additional accredited providers participate in the AGDIS, and that clarity on future interoperability requirements would be beneficial to support investment.

Currently only one ISP participates in the AGDIS (myID), alongside one accredited identity exchange provider (Identity Exchange), 2 accredited attribute service providers (RAM, myGov) and a range of participating Commonwealth and State and Territory relying parties.

Charging – *setting out fees and charges for accreditation and transactions within the AGDIS*

Stakeholders reiterated their view that charging arrangements associated with the accreditation scheme and the AGDIS should be settled as soon as possible, to provide certainty for both relying parties and accredited services. This included clarifying whether the accreditation scheme will include any fees, such as accreditation and/or annual

renewal fees, and the extent to which private sector accredited digital ID service providers will be able to charge for their services in the AGDIS.

The Digital ID Act provides for the Digital ID Rules to be made to enable the Digital ID Regulator to charge fees (including a nil amount) for activities performed either directly by or on behalf of the Digital ID Regulator while carrying out its duties or exercising its powers under the Digital ID Act. However, the Digital ID Act does not allow these fees to involve the charging of individuals for the creation or use of a Digital ID.

At present, there are no fees or charging associated with the Digital ID framework.

Holding information outside Australia

The Digital ID Rules apply to accredited Digital ID providers within the legislated AGDIS, which presently includes only government agency providers. These accredited providers do not store personal information offshore. Existing government policy regarding transferring information outside of Australia continues to apply to all Australian Government agencies participating in the AGDIS.

Anticipating future private sector participation with the AGDIS, the Digital ID Act allows for the Digital ID Rules to make provisions regarding the holding, storing, handling or transfer of information outside Australia by accredited entities participating in the AGDIS.

Stakeholders have put forward a range of views in relation to this subject.
The Government will continue to engage with stakeholders on the matter as part of the development of any future Digital ID Rules. The Government will need to consider the overall impacts on privacy and security, as well as the interactions with Australia's broader policy settings for the handling and storage of data. This includes any Privacy Act amendments being considered by the Australian Parliament (refer Privacy and Other Legislation Amendment Bill 2024) and any consequently amendments to the Australian Privacy Principles (APP). These policy settings include, but are not limited to:

- the APPs, which set out requirements for the cross-border disclosure of personal information (noting that accredited entities must be subject to the APPs, a comparable state or territory framework, or an equivalent agreement with the Commonwealth),[2] and
- the policies that apply to the handling of data by Commonwealth agencies, including the Information Security Manual produced by the Australian Cyber Security Centre, the Protective Security Policy Framework, and the Hosting Certification Framework.

[2] More about the Privacy and Other Legislation Amendment Bill 2024 Part 6 – Overseas disclosures of personal information and Part 6 – Overseas data flows is at: www.aph.gov.au/Parliamentary_Business

APP 8 regarding cross-border disclosure of personal information still applies to all Government agencies within AGDIS, along with all existing government policies on transferring information abroad. These obligations apply irrespective of the country where the relevant personal information is stored and applies to accredited entities within AGDIS, who must also comply with strict protective security obligations under the Accreditation Rules to ensure personal information is secure and protected.

Protective security risk management and rule upkeep

Throughout the 2024 consultation, stakeholders frequently emphasised the importance of ensuring the security requirements in the Accreditation Rules are kept updated to address evolving risks, technology, and emerging threats such as artificial intelligence and potential quantum computing-based cybersecurity threats.

Stakeholders noted overlap with other legislation such as under the Commonwealth SOCI Act and Consumer Data Right (CDR) legislation; noting that evidence provided to regulators in other regulatory schemes may be used to meet requirements in the Accreditation Rules, particularly protective security requirements. While this is already enabled in the current rules, further work to support mutual recognition across regulatory schemes is underway.

The rules relating to protective security are to be continuously maintained to ensure that they remain current and appropriate for existing and emerging risks.

The Government is aware that there are some closely related policy initiatives that may be placing similar requirements on a business. However, these requirements are closely calibrated to the policy outcomes they are intended to deliver and are considered appropriate at this time. As the initiatives move forward, scope to better align and reduce duplication will be considered.

Identity proofing options and fraud mitigation strategies

There was strong support for Commonwealth, State and Territory governments to explore alternative proofing options which may enable individuals who do not have and are unable to obtain the required ID documents to create a digital ID.

To assist fraud mitigation, there were suggestions from stakeholders that in the short-term, digital ID services could expand the use of technology that is commonly used in the private sector to verify that physically presented identity documents have not been tampered with and are legitimate. This could include expanding the use and application of electronic Identity Document Verification Technology (eIDVT), which is able to be used as a biometric matching technology option in the rules now but in future could be expanded to other use scenarios to assist with fraud mitigation. Though further policy work is necessary before adopting this technology in the rules and standards, it may

provide enough confidence that the document is legitimate to negate the need to check the veracity of that document with its issuer. This could allow some additional documents to be permitted as part of digital ID identity proofing processes.

Other supporting instruments

Digital ID Transitional Rules

The Transitional Rules deem listed entities to be approved as accredited entities, or to be approved to participate in the AGDIS, or both. The rules specify any conditions of an entity's accreditation, entities and relying parties' participation. Generally, these conditions set out the scope of the service that is accredited, participating in the AGDIS (or both) and how the services must be connected to the AGDIS (if relevant). Conditions may also permit accredited entities or AGDIS participants to disclose restricted attributes for the purposes listed in their condition.

The Transitional Rules were subject to targeted consultation with existing accredited entities, and service entities participating in the AGDIS to ensure the accuracy of the entities listed in the rules, and confirm the correct conditions on their services to apply on commencement.

Phasing Determination

The Minister can manage the expansion of AGDIS to entities beyond the kinds of Commonwealth entities specified in subsections 61(a) and (b) of the Digital ID Act, and other Commonwealth and State and Territory entities listed in the Transitional Act and the Transitional Rules.

Section 60 of the Digital ID Act allows the Minister, by legislative instrument, to determine the kinds of entities that may apply to the Digital ID Regulator for approval to participate in the AGDIS. The Minister has the flexibility to implement the phasing in any manner, including specifying whether entities are relying parties or accredited entities, and whether they belong to the public or the private sector.

The Phasing Determination allows State and Territory government entities not already listed in the Transitional Rules to apply to the Digital ID Regulator for approval to participate in AGDIS as either accredited entities or relying parties. The Determination was developed in consultation with States and Territories.

A phased approach to expanding the AGDIS ensures controlled and secure integration of entities into AGDIS and allows the Government to manage potential risks associated with the integrating entities with differing operational practices and security needs. This approach allows the system's infrastructure and security measures to be robust and adaptable, accommodating a diverse range of participants while maintaining

the system's integrity. It also allows for the development of key policies ahead of each phase, such as those relating to charging, redress, and liability.

The Minister cannot revoke the determination but can vary the determination to add additional entities or correct errors. This provides stability and certainty for entities authorised to apply for participation.

Conclusion

The Government thanks stakeholders for actively participating in the consultations, informing the making of the rules and data standards.

The Government will continue to progress the necessary rules and standards needed for Digital ID including the expansion of the AGDIS to the private sector.

The Government will collaborate with the Data Standards Chair (appointed under the Digital ID Act), to ensure the rules align with the data standards as required.