Australian Government
Department of Finance

14 July 2026

Statutory Review of the Digital ID Act 2024 – Issues Paper

Contents

Glossary

Accreditation Scheme	The voluntary accreditation scheme established under the *Digital ID Act 2024*. It is open to all government and private sector providers across the economy.
Attribute	An attribute of an individual means information that is associated with the individual, and includes information that is derived from another attribute (for example, the attribute of being over 18 years old is information derived from an individual's date of birth).
Attribute Service Providers	Provides a service that verifies and manages an attribute of an individual.
Australian Government Digital ID System (AGDIS)	The AGDIS means the digital ID system overseen and maintained by the Digital ID Regulator. It is a secure, voluntary system for individuals to verify their identity to access certain government services. From December 2026, private entities can apply to join the AGDIS.
Identity Exchange Providers	Provides a service that conveys, manages and coordinates the flow of data or other information between participants in a digital ID system.
Identity Service Providers	Generates, manages, maintains or verifies information about the identity of an individual to create or manage a digital ID.
Relying Party/ies	An entity that relies, or seeks to rely, on an attribute of an individual that is provided by an accredited entity to provide services or enable individuals to access services.

Statutory Review of the Digital ID Act 2024

The Minister for Finance, Senator the Hon. Katy Gallagher has initiated a statutory review of the operation of the *Digital ID Act 2024* (the Act) and appointed Ms Roxanne Kelley PSM to lead the review.

Purpose of the Review

Section 162 of the Act requires a review of the Act to be undertaken within two years of the Act's commencement, which occurred on 30 November 2024. This requirement aims to ensure timely consideration as to whether the Act is operating as expected.

The Review will allow an independent assessment of the operation of the Act and whether the Act is achieving its objectives.

The Reviewer must provide a written report to the Minister for Finance. A copy of the report must be tabled in each House of the Parliament within 15 sitting days after the Minister receives it.

Terms of Reference

The Review will assess the operation of the Act, including whether it is operating to achieve the objects of the Act, and whether the legislation would benefit from any amendments to improve the operation of the legislative framework particularly in the context of changes in the broader digital and data environment and developments in related legislation.

The objects of the Act, set out in section 3, are to:

- provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity in online transactions with government and businesses
- facilitate the inclusion of individuals in digital society by supporting the provision of digital ID services that are accessible for individuals who experience barriers in using such services
- promote privacy and the security of personal information used to verify the identity or attributes of individuals
- facilitate economic benefits for and reduce burdens on the Australian economy by encouraging the use of digital IDs and online services
- promote trust in digital ID services amongst the Australian community.

The matters the Review will consider, and may make findings and recommendations about, include whether:

- The digital ID legislation is operating as intended to achieve its objects.
- The digital ID legislation is operating to support increased digital ID uptake by individuals, businesses and government services, including supporting the modernisation of service delivery.

- The digital ID accreditation scheme and its associated regulatory and oversight settings are effective and proportionate, including to support expanded participation in the accreditation scheme and to advance the objects of the digital ID legislation.
- The regulatory and oversight settings for the Australian Government Digital ID System (AGDIS) support government services using digital ID when providing services and support private sector use of government digital ID services.

For the purposes of the review, the Act includes *Digital ID Rules 2024*, *Digital ID (Accreditation) Rules 2024*, *Digital ID (AGDIS) Data Standards 2024*, the *Digital ID (Accreditation) Data Standards 2024* and the Regulatory Powers Act as it applies in relation to the Act.

Consultation Process

The Review will be informed by consultation with representatives from government stakeholders, industry/business stakeholders, and other interested parties. Feedback can be provided to the Review through written submissions or meetings with the Reviewer or supporting Secretariat.

This issues paper provides additional context about the focus of the Review to assist stakeholders and interested parties.

Stakeholders and interested parties are invited to make submissions on any or all issues raised by the Terms of Reference. Below are the questions the Review is particularly interested in exploring to understand how the Act is operating and the opportunities for making the system work better.

1. Is the Act and supporting legislative framework operating to advance its objects?

The Review is seeking feedback on whether the Act is operating to achieve these objects, in particular:

- Supporting the uptake of digital IDs by individuals.
- Promoting the privacy and security of personal information used to verify the attributes of individuals.
- Facilitating the inclusion of individuals in digital society by supporting the provision of digital ID services that are accessible for individuals who experience barriers.
- Achieving economic benefits and reducing burdens on the Australian economy.

2. Is the legislation supporting the uptake of digital ID and improving service delivery?

The review is seeking feedback on whether:

- Entities are experiencing any barriers to introducing digital ID into systems or processes to verify identity.
- The legislative framework sufficiently supports innovation in how digital ID services are being delivered. This includes whether the legislation is sufficiently technology neutral to support advancements or alternatives in technology used to deliver services.

- The legislative framework is readily adaptable to changes in the broader data and digital landscape.
- There are barriers outside the digital ID legislative and operating framework that affect participation in the digital ID system. For example, is there regulation, government policy or industry expectations that affect how digital ID is or can be used in the Australian economy.

3. Are the regulatory and oversight settings for the Accreditation Scheme effective and proportionate?

The Review is seeking feedback on whether:

- The costs involved in applying for and maintaining accreditation, and the necessary investment in IT infrastructure create any barriers to entry or expansion.
- The regulatory and oversight settings promote trust in accredited entities and strike the right balance in meeting community expectations of privacy and security and business investment and commercialisation.
- The Accreditation Scheme creates an environment that supports and fosters innovation in service delivery.
- There are opportunities to reduce regulatory complexity and burdens.
- Mutual recognition or streamlined accreditation with other comparable accreditations schemes would achieve the Act's objects.
- Voluntary accreditation is the best regulatory model for regulating digital ID service providers in Australia.
- The privacy settings in the Digital ID legislative framework (comprising the Act, the rules and data standards) strike the right balance and whether the additional privacy safeguards in the Act remain appropriate given reforms to the *Privacy Act 1988* that commenced in December 2024.

4. Are regulatory and oversight settings for the Australian Government Digital ID System supporting government use of digital IDs and private sector use of government digital ID services?

The Review seeks feedback on whether:

- The costs involved in applying for and maintaining approval to participate in AGDIS, including costs involved with uplifting data environments, required policies and procedures, and demonstrating an ability to comply with the regulatory framework create any barriers to entry or expansion.
- There is sufficient clarity around the regulatory scope of the AGDIS and the roles of the Digital ID Regulator and System Administrator.
- The additional regulatory obligations on AGDIS participants balances the protections for individuals with government and business needs to modernise service delivery and reduce risks of cyber-attack and fraudulent conduct.
- The consequences for non-compliance by entities participating in AGDIS are appropriate.

5. Are there options for longer term reform?

The Review seeks feedback on whether:

- The legislative framework can effectively support evolving methods of digital ID and identity verification.
- The legislative framework could be more principles-based and maintain an appropriate level of privacy and security for individuals and businesses.
- There are alternative regulatory and oversight models that could continue to maintain an appropriate level of privacy and security for individuals and businesses.
- Alternatives (e.g. digitalised identity credentials or verifiable credentials) could achieve the same policy objectives as digital ID.

How to make a submission

Stakeholders and interested parties are invited to comment on the issues raised in this paper and provide any other feedback on the Act by **14 August 2026**. Submissions may be lodged electronically or by post, with electronic lodgement being preferred.

For accessibility reasons, please submit electronic responses in a Word or RTF format. An additional PDF version may also be submitted.

If you choose to provide a submission, information in your submission may be used to inform the Reviewer's findings and recommendations and may be included in the Reviewer's report to the Minister. Information (including name and address details) may also be made available to the public on the Department of Finance website by publishing your submission or a summary of your submission, unless you indicate that you would like all or part of your submission to remain confidential. Respondents who would like part of their submission to remain confidential should provide this information marked as such in a separate attachment, together with the reasons the relevant material should remain confidential. Parties are encouraged to contact the Department of Finance for further information and advice before submitting such material.

There can be circumstances where the Department of Finance may be required to disclose certain information, for example, documents required to be released under the *Freedom of Information Act 1982*. In such circumstances, the Department of Finance will consult with you before making a decision to disclose any or all of your confidential submission.

Submissions should be submitted via the consultation page, which can be accessed at **DigitalIDSystem.gov.au/Have-Your-Say**.

Background

Digital ID is a major economy-wide reform with significant economic, security and privacy benefits for individuals and businesses.

The genesis of the Digital ID legislation lay in the *Report of the Financial System Inquiry* (2014) (the Financial Systems Inquiry) which recognised the potential benefits of a whole of economy Digital ID system. The Financial System Inquiry set out the policy problems to be addressed as:

- **Fragmentation** – Australia's identity system was fragmented, with some parts operated by the Commonwealth, or State or Territory Governments (e.g. the issuance of core identity documents) and a range of identity practices occurring across the private sector

- **Digitalisation of the economy** – as transactions have moved online, there has been more demand for identity solutions that can work online, rather than face to face. The Financial Systems Inquiry also suggested that digital identity solutions would improve efficiency and security
- **Promoting competition between identity providers** – the Financial System Inquiry considered that competition between identity service providers would promote innovation

To address these policy problems, the report recommended the Australian Government develop a national strategy for a federated-style model of trusted digital identities in which public and private sector identity service providers would compete to provide identity services, enhancing consumer choice, privacy, innovation and system efficiency.

The Trusted Digital Identity Framework was introduced in response, establishing an unlegislated accreditation scheme for digital ID service providers and rules for participation in the AGDIS. Legislating both the accreditation scheme and the AGDIS was the logical next step to ensure both initiatives could be expanded effectively and safely to ensure the benefits of digital ID are realised across the economy.

The Digital ID Act commenced on 30 November 2024 and defines a digital ID as a distinct digital representation of an individual that enables the individual to be sufficiently distinguished when interacting online with services.

A digital ID is not a digital version of an individual's existing identity documents, e.g. a digital ID is not a digital driver licence. An individual can create a digital ID with an identity service provider. When creating a digital ID, identity service providers verify an individual's identity by checking details against official records held by government agencies. Once set up, it provides individuals with a convenient, re-usable way to verify who they are when transacting online, without having to repeatedly provide copies or details of their most sensitive ID documents.

The commencement of the Act introduced two reforms to support the expansion of Australia's Digital ID System on a whole of economy basis:

- It strengthened a voluntary **accreditation scheme** for three kinds of digital ID service providers—**identity service providers**, **attribute service providers** and **identity exchange providers**—in the public and private sectors; and
- It provided a legislative basis for expanding the existing **Australian Government Digital ID System (AGDIS)** to include digital ID services provided by States and Territories and, from December 2026, to private sector organisations that choose and are approved to participate in the system as either providers or users (i.e. **relying parties**) of accredited Digital ID services.

The Act does not apply to digital ID services providers who choose not to accredit their digital ID services or to relying parties who use accredited digital ID services outside of the AGDIS.

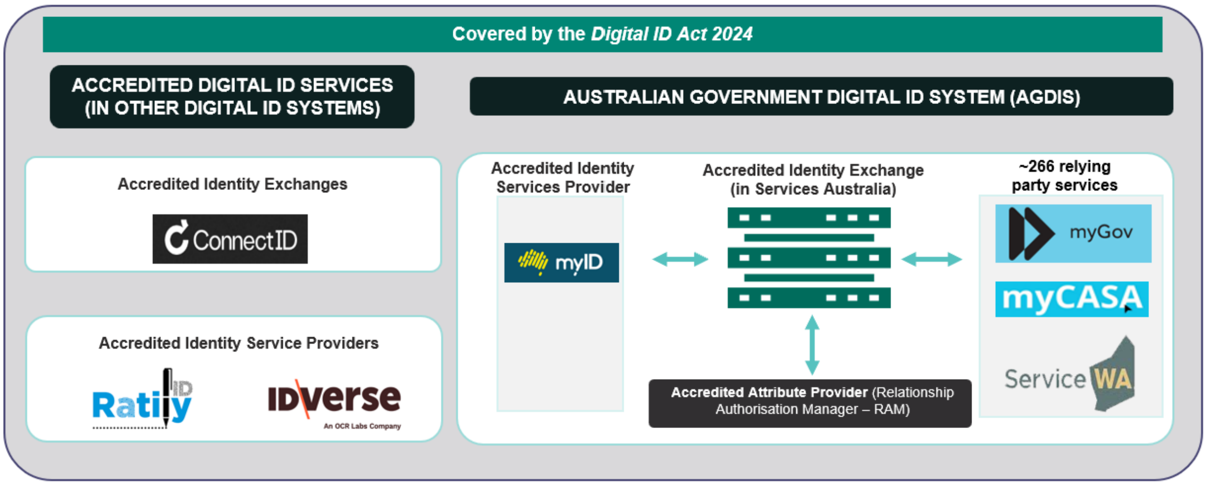
Progress to date

Australians are embracing Digital ID and for good reason.

As of May 2026, there are 39 government agencies operating in the AGDIS, offering 266 government services which can be accessed by using the Commonwealth digital ID (myID). Between 1 June 2025 and 30 May 2026, there were more than 111 million authenticated transactions through the AGDIS – up from 43 million in the previous 12-month period, an increase of 258 per cent.

The digital ID services currently offered in Australia include:

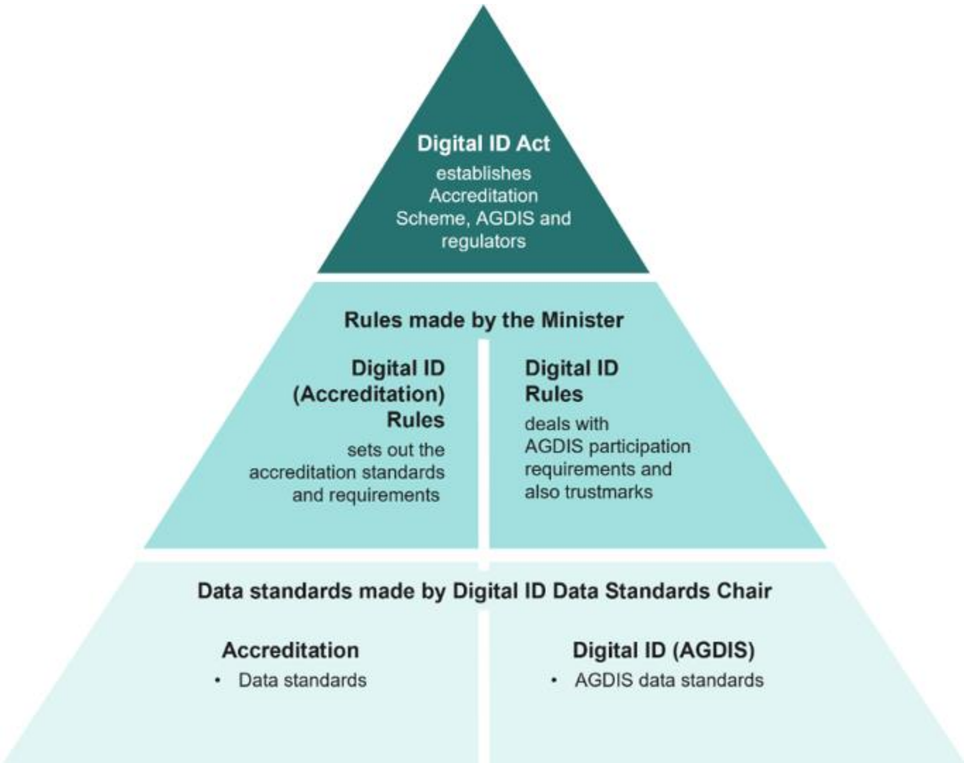
- myID – the Commonwealth's digital ID service provider (operated by the ATO)
- An accredited private sector identity exchange – ConnectID
- An accredited government identity exchange – operated by Services Australia
- Accredited private sector identity service providers – Makesure and IDVerse
- Accredited government attribute providers – operated by the ATO and Services Australia



The Australian Government is investing $654.3 million over four years from 2026–27, and $166.7 million ongoing to expand the use of digital ID across the economy—building on the $465.8 million already committed since 2023. With the Act now in effect, government and private sector services can seek accreditation of their Digital ID services. And, from December 2026, businesses will be able to apply to participate in the AGDIS.

Legislative Framework

The legislative framework supporting Australia's digital ID system and subject to this review comprises the Act, two sets of rules and two sets of data standards which are all legislative instruments, and the Regulatory Powers Act as it applies in relation to the Act.



Supporting legislative instruments

The legislative instruments support the implementation and ongoing administration of the legislation.

Rules

The Minister can make rules about a range of matters related to the Accreditation Scheme and the Australian Government Digital ID System (AGDIS). The rules are disallowable legislative instruments.

The Accreditation Rules apply to digital ID service providers (identity service providers, attribute service providers and identity exchange providers) who choose to obtain accreditation, regardless of whether they participate in the AGDIS. The Accreditation Rules detail application processes and requirements for privacy, security, accessibility, and other obligations that apply to accredited entities.

The Digital ID Rules apply to entities who participate in the AGDIS and outline the requirements for those wanting to participate (both accredited entities and relying parties). The Digital ID Rules provide for a redress framework and specifies how the digital ID trustmark can be used.

Data standards and service levels

The Digital ID Data Standards Chair is responsible for making standards for various matters relating to the AGDIS and the Accreditation Scheme, including data standards, design standards and service level determinations. The data standards are non-disallowable legislative instruments.

Accreditation Scheme

The Accreditation Scheme is designed to promote the growth of, and trust in, digital ID services throughout the economy. The Accreditation Scheme is voluntary and open to government and private entities. Accreditation is available for different kinds of entities providing digital ID services:

- attribute service providers, who deliver services that verify and manage specific attributes of an individual
- identity service providers, who deliver services that generate, manage, maintain or verify information about an individual's identity, and may also generate, bind, manage or distribute authenticators, including those created by the individual
- identity exchange providers, who facilitate the secure flow of information by conveying, managing and coordinating data exchanges between participants in the Digital ID System

If another kind of digital ID service becomes available, this kind of service may be prescribed in the Accreditation Rules as a service of a kind that can be accredited.

The Accreditation Scheme requires accredited entities to ensure their accredited services adhere to certain privacy, security, fraud, systems testing, usability, and accessibility rules and standards – all with the aim of promoting public trust in those services.

Accreditation is granted to an entity in relation to the specified digital ID services (i.e. accreditation is granted to be an accredited attribute service provider, an accredited identity service provider or an accredited identity exchange provider), and not in relation to the entity's broader services, functions or activities.

- An entity, when applying for accreditation, must clearly identify and delineate the 'DI data environment', being the data environment that manages the digital ID services. Information within the accredited DI data environment must be managed in compliance with the Act and the Accreditation Scheme.
- This means that if an entity handles personal information to provide its accredited digital ID service, and also handles personal information to provide other services, functions or activities, the entity will have different regulatory obligations in relation to the collection, use and disclosure of the personal information under the Act and under the *Privacy Act 1988*, even where this may involve the same personal information.

Entities which apply for accreditation must apply using an approved form, have commissioned various independent assurance assessments and testing of their accredited services, and have evidence to demonstrate or attest to such assessments and testing being conducted. Once their services are accredited, entities are required to demonstrate ongoing compliance with the Accreditation Scheme and the regulatory obligations (particularly as they relate to compliance with the privacy, security, fraud, systems testing, usability, and accessibility rules and standards). Entities are required to undertake an annual review of their accredited services and relevant data environment and conduct regular assurance assessments and testing of systems and controls and provide reports to the Digital ID Regulator (the ACCC).

Accredited entities can use and display the Digital ID Accreditation Trustmark. The Trustmark helps consumers identify accredited providers who have demonstrated they meet the accreditation standards and provide trustworthy digital ID services that protect people’s personal information.

It is important to note that the Accreditation Scheme is only available to entities providing digital ID services, not to relying parties which use those services. For digital ID service providers who wish to join the Australian Government Digital ID System, accreditation is mandatory.

Privacy Protections

The Act has privacy protections as part of its design and these are key to building and maintaining trust in the creation and use of digital IDs.

For example, the Act uses the concept of attributes to cover the different types of personal information that may be used in accredited services. Section 11 of the Act prescribes certain types of personal information as restricted attributes (such as government identifiers or health information) and places certain restrictions over the use of these attributes. Section 44 of the Act further prescribes certain other types of personal information as prohibited attributes (such as racial or ethnic origin) which may not be used in accredited services.

Chapter 3 of the Act applies a range of additional privacy safeguards on accredited services that build upon existing privacy laws. The additional privacy safeguards include:

- requirements for express consent to share certain personal information with relying parties
- requirements to deactivate a digital ID at the request of an individual
- prohibitions on the use of single identifiers between entities
- prohibitions on the use of personal information for data profiling and the use of information for direct marketing purposes
- restrictions on the use and retention of biometric information, including a prohibition on one-to-many biometric matching
- additional safeguards over law enforcement access to personal information held by accredited entities.

Additional requirements and obligations in the Act’s supporting rules and data standards further enhance the privacy settings, including a data minimisation principle which discourages the unnecessary collection and disclosure of personal information using accredited services.

Australian Government Digital ID System (AGDIS)

The AGDIS is a network of entities which, together, provide individuals and businesses with a voluntary, secure, and convenient way to verify their identity to access government services.

The AGDIS provides a mechanism to apply certain safeguards and other policy settings over the operation of accredited Digital ID services *that involve government agencies*, as providers or relying parties. These safeguards are over and above those within the Accreditation Scheme that apply to accredited entities that operate in other digital ID systems.

The Act places additional requirements on accredited entities and relying parties who participate in the AGDIS to ensure their services protect the privacy and security of digital ID users. For example, accredited entities that hold an approval to participate in AGDIS (or whose approval has been suspended or revoked) must destroy or de-identify any personal information obtained through the provision of its services in the AGDIS, and there are strict conditions on the circumstances in which participating relying parties can collect restricted attributes.

The AGDIS is currently based around the Commonwealth accredited identity service provider (myID), accredited attribute provider (Relationship Authorisation Manager, or “RAM”) and accredited identity exchange (operated by Services Australia) which facilitates the flow of information between participating accredited services and relying parties. Some Commonwealth, State and Territory agencies participate in the AGDIS as relying parties and use myID and/or RAM to deliver online services to individuals and businesses.

Entities participating in the AGDIS must hold an approval granted by the Digital ID Regulator. Approval to participate is subject to conditions. For example, a participating accredited entity can only provide the service it is accredited and approved to provide by the Digital ID Regulator. The Digital ID Regulator can approve an entity to participate in the AGDIS, as well as suspend and revoke that approval and the System Administrator is responsible for the day-to-day operation of the AGDIS – both roles are described in more detail below.

A key feature of the AGDIS is that use of a digital ID to access services provided by participating relying parties through the AGDIS is voluntary for individuals. For example, the Act requires relying parties participating in the AGDIS to provide an alternative way for a person to access a service without using a digital ID, unless the person is accessing a service on behalf of another entity in a business or professional capacity. These alternative means must be reasonably accessible and not result in a service being provided on substantially less favourable terms.

Entities (but not Commonwealth entities) can apply to the Digital ID Regulator for an exemption to the voluntariness obligation. The Digital ID Regulator may grant an exemption if it is satisfied it is appropriate to do so and must have regard to whether the exemption would unduly undermine access to services of the kind for which the exemption is sought. For example, the Digital ID Regulator may be satisfied it is appropriate to grant an exemption if the participating relying party is a small business, provides services or access to services solely online or provides services or access to services in exceptional circumstances.

Participants in the AGDIS are required to report certain incidents (such as digital ID fraud and cyber security incidents) and may be required to provide certain redress measures to affected individuals. These requirements help maintain the availability, performance and integrity of the AGDIS, and further enhance the security and convenience for the individual.

The Act enables the AGDIS to expand beyond the Commonwealth, first by allowing the reciprocal use of State and Territory digital ID service providers and, from December 2026, the use of private sector digital ID service providers. The expansion of the AGDIS to the private sector will also enable businesses to apply to the Digital ID Regulator to participate as relying parties. The intent here is to provide individuals with choice about which digital ID they use to access government services online, and to promote competition and innovation among participating entities.

Importantly, the AGDIS sits alongside and does not displace other digital ID systems that operate within the private sector – for example, a private digital ID service provider may wish to become accredited to promote trust with potential customers but not want to participate in the AGDIS. Accredited private sector entities wishing to participate in the AGDIS may continue to offer services outside the AGDIS as well, provided the entity can demonstrate to the Digital ID Regulator how it will manage its services and data environments operating in and outside the AGDIS. This means that businesses which provide accredited services, or which use accredited services as relying parties, within and outside the AGDIS may be subject to different regulatory requirements.

Regulation and Oversight

Oversight is aligned with the government agency who has the relevant regulatory responsibility:

- the Digital ID Regulator (the ACCC) focuses on accreditation and approving entities to participate in AGDIS as well as compliance and enforcement,
- the Information Commissioner provides independent oversight of enhanced privacy protection obligations, and
- the System Administrator manages day-to-day operation of the AGDIS.

This multi-agency model promotes stronger accountability, reduces conflicts of interest, and supports a balanced approach to security, privacy, and operational stability.

The Department of Finance is responsible for digital ID policy and administration of the Act.

Digital ID Regulator

The Digital ID Regulator is the Australian Competition and Consumer Commission (ACCC).

The Digital ID Regulator is responsible for administering the Accreditation Scheme, including accrediting entities to provide digital ID services, and for overseeing and maintaining the AGDIS, including approving accredited entities and relying parties to participate in AGDIS. The Digital ID Regulator is also responsible for promoting compliance and taking enforcement action in relation to matters other than the privacy safeguards.

The Digital ID Regulator maintains a register of accredited entities and a register of entities approved to participate in AGDIS.

Information Commissioner

The Information Commissioner is given an expanded role under the Act and is responsible for providing oversight of the additional privacy safeguards, including complaint-handling, investigations and taking enforcement action, performing Notifiable Data Breach scheme functions in relation to the digital ID system and undertaking assessments of Digital ID system compliance by accredited providers.

System Administrator for the AGDIS

The Chief Executive Centrelink is the System Administrator.

The System Administrator for the AGDIS has functions related to assisting entities participating in the AGDIS, and managing the availability of the AGDIS, fraud and cyber incidents in the AGDIS, and operational risks.

A Memorandum of Understanding (MoU) between the Office of the Australian Information Commissioner (OAIC), the Chief Executive Centrelink and the ACCC support the parties to carry out their independent digital ID functions by facilitating cooperation, consultation and legally permitted information sharing between the parties.

The Broader Context

The Act is operating in the broader digital and data environment and relevant legislative developments, including:

- the Australian Government's 2023-2030 Australian Cyber Security Strategy which established a framework for the Australian Government to take action to uplift Australia's cyber security resilience and maturity and help realise the Australian Government's vision of becoming a world leader in cyber security by 2030. Expanding the adoption of Digital ID across government and private sectors is highlighted in the Cyber Security Strategy as an action critical to increasing productivity, security and consumer protection.[1]
- the Consumer Data Right (CDR) which provides consumers the right to share their own data between service providers. The CDR is currently active in the banking and energy sectors. As digital ID expands across the economy, it is expected that an increasing range of digital transactions will involve a combination of data that is regulated by the CDR and Digital ID schemes; and that an increasing range of entities will become regulated under both schemes.
  - The CDR and Digital ID both involve accreditation schemes with additional privacy safeguards and other requirements relating to the handling of personal information. Alignment between the requirements of both regimes could reduce the regulatory impact on entities operating in both schemes or transactions involving CDR and Digital ID data.
- reforms to the *Privacy Act 1988* which came into effect on 10 December 2024 and which progressed 23 proposals from the Government Response to the Privacy Act Review Report[2].
  - The Act contains additional privacy safeguards that apply to all accredited entities and that build on the privacy safeguards contained in the *Privacy Act* (or equivalent state or territory laws).
- The statutory reviews of the *Identity Verification Services Act 2023 (IVS Act)* were initiated by the Attorney-general in June 2026. These consists of an Interim Review and the Act Review. The Interim Review will consider the adequacy and operation of the privacy protections and security requirements in the IVS Act and associated instruments. The Act Review will consider the operation of the IVS Act, and the provision of the IVS more broadly
  - The IVS Act regulates the operation of the Document Verification Service and the Face Verification Service (two of the identity verification services), which are used to verify

[1] Action Plan for Horizon 2 of the 2023-2030 Australian Cyber Security Strategy, p 12.
[2] Review of the Privacy Act 1988 | Attorney-General's Department

the authenticity of an individual's identity documents (e.g. drivers' licence, passport) when setting up a digital ID, such as a myID.

- New and emerging technologies, such as verifiable credentials which are secure digital versions of credentials such as digital driver licences that are issued by some States and Territories. Verifiable credentials offer alternative ways to verify information rather than using Digital IDs and may become more commonplace as demand grows for trusted solutions which not only verify a person's identity but also verify specific attributes or qualifications (e.g. drivers' licences, proof of age).

Key consultation points for discussion

Stakeholders and interested parties are invited to make submissions on any or all issues raised by the Terms of Reference. Below are the questions the Review is particularly interested in exploring to understand how the Act is operating and the opportunities for making the system work better.

1. Is the Act and supporting legislative framework operating to advance its objects?

The objects of the Act, set out in section 3, include providing individuals with secure, convenient, voluntary and inclusive ways of verifying their identity in online transactions, promoting privacy and security of personal information used to verify identity and promoting trust in digital ID services amongst the Australian community. The objects also include facilitating economic benefits and reducing burdens on the Australian economy by encouraging the use of digital IDs and online services.

The Review is seeking feedback on whether the Act is operating to achieve these objects, in particular:

- Supporting the uptake of digital IDs by individuals.

A number of the Act's objects are centred around protections and convenience for the individual. The Act includes additional privacy protections, requirements to ensure creation and use of a digital ID is voluntary, and obligations to ensure services and systems are safe and secure. This is intended to promote trust by individuals in creating and using a digital ID and encourage using a digital ID instead of alternative and less secure methods of sharing identity information.

- Promoting the privacy and security of personal information used to verify the attributes of individuals.

Entities participating in the AGDIS are required to report digital ID fraud and cyber security incidents to the System Administrator. Data from the Office of the System Administrator indicates that the number of reported fraud and security incidents is less than 1% of all digital ID (in this case myID) transactions within the AGDIS. The level of fraud associated with biometrically verified myIDs is even lower – with no reported compromise of IP3 (Strong) level myIDs to date.

- Facilitating the inclusion of individuals in digital society by supporting the provision of digital ID services that are accessible for individuals who experience barriers.

According to the Australian Digital Inclusion Index,[3] approximately one in five Australians face significant barriers to accessing digital services. The Act includes provisions to support individuals who are facing barriers accessing digital ID services, including alternative proofing methods to enable those individuals without, or without access to, traditional identity documents to create a digital ID and use it to gain access to online services.

- Achieving economic benefits and reducing burdens on the Australian economy.

The Act is intended to enable secure and convenient identity verification for online services. For individuals, this is intended to reduce burdens when needing to interact with services,

[3] https://digitalinclusionindex.org.au/

e.g. government services, by allowing identity verification without sharing of identity documents through other less secure methods, and enabling accessing services when convenient for the individual, rather than during open hours for a shop front or call centre.

For business, digital ID can increase productivity and reduce burdens by reducing manual verification processes, reducing costs associated with securely holding personal and sensitive information and increase productivity opportunities through increased automation and improved service delivery.

Research done by the Department of Finance found that using a digital ID and digital ID services could reduce identity verification time by up to 70–90% in use cases requiring multiple checks, such as e-conveyancing or rental applications, by replacing repeated manual document handling with near instant digital verification.

For example, in March 2025, a 12-month pilot was undertaken using Digital ID and the Consumer Data Right (CDR) in rental applications to identify the potential benefits and use cases for digital ID. The pilot successfully concluded on 31 March 2026 and showed that Digital ID and the CDR can eliminate oversharing of personal documents – including drivers' licences, passports, bank statements and payslips – for rental applications. The pilot also showed real estate businesses could save around $150 per rental listing and up to 70 hours each month by reducing the amount of sensitive data they collect.

2. Is the legislation supporting the uptake of digital ID and improving service delivery?

The Act operates within the broader data and digital environment, with advances in technology changing how services are being delivered, including their efficiency and effectiveness as well as changing societal expectations around how and when services can be accessed.

The benefits of a digital ID system and the supporting legislative framework will be fully realised when using a digital ID to verify an individual's identity becomes the most convenient and accepted method of identity verification. This needs an increase in the number of accredited service providers to offer individual's choice of digital ID provider, as well as increasing the range of attributes that can be verified through accredited providers.

Having trust in the system – individuals trusting that their digital ID is safe and secure, and businesses trusting that using digital ID services will reduce instances of data breaches and fraud as well as meeting different regulatory requirements for identity verification – is essential for the ongoing uptake of digital ID and encouraging governments and businesses to design modes of service delivery that adapt to the evolving environment.

There is an upward trend in the use of digital ID to access government services.

- For individuals, there is an increase in the number of individuals creating and using the Australian Government's digital ID, myID, to access government services online. This potentially demonstrates individuals are increasingly trusting digital ID as a safe, secure and convenient way to use online services.
- For government services, there is an increase in the number of government services accessing the AGDIS and using myID, or the accredited attribute RAM.

The review is seeking feedback on whether:

- Entities are experiencing any barriers to introducing digital ID into systems or processes to verify identity.
- The legislative framework sufficiently supports innovation in how digital ID services are being delivered. This includes whether the legislation is sufficiently technology neutral to support advancements or alternatives in technology used to deliver services.
- The legislative framework is readily adaptable to changes in the broader data and digital landscape.
- There are barriers outside the digital ID legislative and operating framework that affect participation in the digital ID system. For example, is there regulation, government policy or industry expectations that affect how digital ID is or can be used in the Australian economy.

3. Are the regulatory and oversight settings for the Accreditation Scheme effective and proportionate?

On commencement of the Act, 6 entities that were previously accredited under the Trusted Digital Identity Framework were deemed accredited by the Digital ID Regulator for 8 services. Since then, there have been no new applications for accreditation and one entity (Australia Post who was accredited as an identity service provider) applied for, and was granted, a revocation of its accreditation status.[4]

The ultimate success of an accreditation scheme depends on its requirements not being overly complex, the cost to obtain and maintain accreditation not too onerous, and that it delivers commercial benefits to those entities who are accredited.

While each accreditation scheme has its own nuance, accreditation schemes used in different sectors of the economy may provide a useful study for how the Accreditation Scheme under the Act could be improved. Presently, it is unclear whether there are benefits to be gained by mutual recognition across schemes or providing streamlined accreditation requirements for those entities already accredited under another scheme.

The Review is seeking feedback on whether:

- The costs involved in applying for and maintaining accreditation, and the necessary investment in IT infrastructure create any barriers to entry or expansion.
- The regulatory and oversight settings promote trust in accredited entities and strike the right balance in meeting community expectations of privacy and security and business investment and commercialisation.
- The Accreditation Scheme creates an environment that supports and fosters innovation in service delivery.
- There are opportunities to reduce regulatory complexity and burdens.
- Mutual recognition or streamlined accreditation with other comparable accreditations schemes would achieve the Act objectives.
- Voluntary accreditation is the best regulatory model for regulating digital ID service providers in Australia.

[4] ACCC, Accredited entities register, <https://www.accc.gov.au/public-registers/digital-id-registers/accredited-entities-register>.

Privacy and other privacy safeguards

Safeguarding the privacy of personal information used in digital ID services is a fundamental design feature of the Act. The Act imposes additional privacy safeguards on accredited entities that build upon existing privacy laws, and the Act, together with the rules and data standards, creates additional privacy protections, including limitations on the collection and disclosure of restricted attributes.

Requiring accredited entities to comply with additional privacy safeguards was considered appropriate to enhance how personal information and digital ID information is handled by accredited entities. Since the Act was made and commenced, there have been reforms to the Privacy Act to further enhance privacy and security protections.

This review is seeking feedback on whether:

- The privacy settings in the Digital ID legislative framework (comprising the Act, the rules and data standards) strike the right balance and whether the additional privacy safeguards in the Act remain appropriate given reforms to the *Privacy Act 1988* that commenced in December 2024.

4. Are regulatory and oversight settings for the AGDIS supporting government use of digital IDs and private sector use of government digital ID services?

The AGDIS comprises a network of government agencies that provide or use digital ID services. It involves an additional layer of governance and regulation, designed to provide additional protections to individuals and promote trust in, and encourage use of, digital IDs as a secure, convenient, voluntary and inclusive method of identity verification.

Accredited entities and relying parties must apply to the Digital ID Regulator (the ACCC) to participate in the AGDIS. The Digital ID Regulator may approve an entity to participate in the AGDIS (or approve with conditions) if the entity demonstrates compliance with Digital ID Data Standards relating to the AGDIS, has shown an ability to comply with the Act, and the Digital ID Regulator is satisfied it is appropriate to approve the entity to participate. The Digital ID Regulator may also consider whether the entity is a fit and proper person.

Before the Digital ID Regulator will approve an entity to participate in AGDIS, the entity will be required to complete testing of their system to confirm it can connect and interoperate with the Services Australia Identity Exchange. The testing process is coordinated by the System Administrator.

From December 2026, private sector accredited entities and relying parties can apply to the Digital ID Regulator to be approved to participate in AGDIS. Implementation continues to support and enable private sector participation in the AGDIS.

The Review seeks feedback on whether:

- The costs involved in applying for and maintaining approval to participate in AGDIS, including costs involved with uplifting data environments, required policies and procedures, and demonstrating an ability to comply with the regulatory framework create any barriers to entry or expansion.

- There is sufficient clarity around the regulatory scope of the AGDIS and the roles of the Digital ID Regulator and System Administrator.
- The additional regulatory obligations on AGDIS participants balances the protections for individuals with government and business needs to modernise service delivery and reduce risks of cyber-attack and fraudulent conduct.
- The consequences for non-compliance by entities participating in AGDIS are appropriate.

5. Are there options for longer term reform?

This Review is being conducted at a time when the Act has been operating for less than two years, and implementation continues in relation to supporting private sector participation in the AGDIS. Given this, it is acknowledged that to understand whether the Act is effectively achieving its objectives, more time is needed to see whether private sector entities can successfully participate in AGDIS and whether there are ongoing changes in the area of digital ID.

However, recognising the evolving data and digital environment, it is important to monitor developments and consider whether the current legislative framework will be able to readily adapt to new use cases, new technologies and new modes of delivering services.

Indeed, as digital technologies evolve and become more sophisticated, there is an important question as to whether the Act is sufficiently designed to respond to these developments. For example, the Minister can prescribe other services that an entity may be accredited to provide in the Accreditation Rules which means that new types of digital ID services may be included as accredited services in the future.

An example of an emerging technology that has potential implications for digital ID are verifiable credentials. Verifiable credentials provide a digital alternative to physical credentials, overcoming the need for credentials to be issued and held in physical form only. Verifiable credentials can be issued digitally in near real-time, securely stored on your phone or other device, and carried with you to be used where and when you need them. Verifiable credentials may also prove useful to underpin other new technologies, such as agentic AI. Recent policy consultation has been undertaken that will help the government to better understand how verifiable credentials might interact with digital ID.

  - The Government has been consulting on proposed Commonwealth policy for the use of verifiable credentials. The consultation provides the opportunity to consider community feedback on proposed positions and will inform further policy development, including the potential formulation of a Commonwealth VC Trust Framework.

The Review seeks feedback on whether:

- The legislative framework can effectively support evolving methods of digital ID and identity verification.
- The legislative framework could be more principles-based and maintain an appropriate level of privacy and security for individuals and businesses.
- There are alternative regulatory and oversight models that could continue to maintain an appropriate level of privacy and security for individuals and businesses.

- Alternatives (e.g. digitalised identity credentials or verifiable credentials) could achieve the same policy objectives as digital ID.