Maddocks

Department of Finance

Privacy Impact Assessment Update No.1

Digital ID Framework

Date of analysis – 16 October 2024

Date of finalisation – 12 November 2024

Contents

Part A Executive Summary

1. Introduction

1.1 The Digital ID Bill 2024 (the **Bill**) was assented to on 30 May 2024. The *Digital ID Act 2024* (Cth) (the **Act**) and the following associated instruments will commence on 1 December 2024 to establish the framework underpinning the Digital ID System:

1.1.1 the Digital ID Rules 2024 (**Digital ID Rules**);

1.1.2 the Digital ID (Accreditation) Rules 2024 (**Accreditation Rules**);

1.1.3 the Digital ID (Accreditation) Data Standards 2024 (**Accreditation Data Standards**); and

1.1.4 the Digital ID (AGDIS) Data Standards 2024 (**AGDIS Data Standards**)

(collectively, the **Draft Rules and Standards**).

1.2 A privacy impact assessment (**PIA**) was undertaken in December 2023, with an Addendum in January 2024 (**Original PIA**), on the:

1.2.1 Exposure Draft of the Digital ID Bill and amendments made to the Bill prior to its introduction in Parliament; and

1.2.2 drafts of the Digital ID Rules and the Accreditation Rules made available for public consultation in September 2023 (**September 2023 versions**).

1.3 In July 2024, the Department of Finance (**Department**) engaged Maddocks to conduct an update to the Original PIA (**PIA Update**) to:

1.3.1 consider proposed changes to the Digital ID Rules and Accreditation Rules since the September 2023 versions (which includes the further drafts made available in May 2024 for public consultation and proposed amendments following consultation);

1.3.2 the proposed Accreditation Data Standards (which includes the draft made available for public consultation in May 2024 and proposed amendments following consultation); and

1.3.3 the proposed AGDIS Data Standards (which were made available for public consultation in July 2024).

1.4 This PIA Update reflects the Department's continuing commitment to a 'privacy by design' approach to developing the framework for the Digital ID System. This PIA Update report considers the privacy impacts of the proposed changes to the Digital Rules and Accreditation Rules, and the proposed Accreditation Data Standards (as at 20 September 2024) and the AGDIS Data Standards (as at 16 October 2024).

2. This PIA Update Process

2.1 Undertaking this PIA Update is consistent with the requirements of the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, which requires agencies to undertake a written PIA for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information which are likely to have a significant impact on the privacy of individuals. However, undertaking a PIA also represents privacy best practice.

2.2 PIAs in respect of proposed new legislation and subordinate legislative and other instruments require a slightly different approach to other PIAs that consider the handling of personal information in projects under an existing legislative regime, which involve an analysis of that handling against Australian Privacy Principles (**APPs**) in the *Privacy Act 1988* (Cth) (**Privacy Act**). This is because the Privacy Act expressly permits the handling of personal information which is 'required or authorised' by an Australian law. For PIA Updates such as this one, which include consideration of proposed new Australian law, the question then becomes whether the proposed Australian law *should* provide that authorisation.

2.3 This PIA Update builds on the Original PIA but does not reconsider issues that were discussed, or recommendations that were made in the Original PIA. This PIA Update also does not cover changes made to the Digital ID Bill 2024, and reflected in the Act, as a result of the Bill's passage through Parliament (which occurred after the date of the Original PIA).

2.4 Like the Original PIA, this PIA Update considers the privacy impacts of the Digital ID System using the framework of the Privacy Act, including the APPs, to provide a baseline consideration of the issues, by applying the principles that sit behind each APP (which are supported by Australian and international privacy best practice).

2.5 We have conducted our analysis on the drafts of the Digital ID Rules, Accreditation Rules, Accreditation Data Standards and AGDIS Data Standards as at the dates specified in paragraph 1.4. We have not considered any further refinement of those drafts after this date.

2.6 Our analysis is based upon the provisions of the Privacy Act, and associated case law and guidance material, as at the date of analysis on the cover page of this PIA report. We have endeavoured to take into account relevant proposed reforms of the Privacy Act discussed in the *Privacy Act Review Report* released by the Attorney General's Department, and the Government's response to the recommendations in that report, and in the Privacy and Other Legislation Amendment Bill 2024. We note that entities subject to the Digital ID Framework may be subject to further measures to protect personal information should any relevant changes to the Privacy Act be enacted.

2.7 In addition, the Department has undertaken consultation processes on the Draft Rules and Standards to support the Act. The Department prepared an extensive Consultation Guide detailing the changes to the draft Digital ID Rules and Accreditation Rules since the September 2023 versions, as part of its May 2024 public consultation process. The Consultation Guide summarised key themes from the September 2023 consultation process. The Consultation Guide also explained the context of the draft Accreditation Data Standards. The Department also prepared 'Your Guide to the Digital ID (AGDIS) Data Standards', to support the public consultation on the AGDIS Data Standards.

2.8 We have had regard to the guides prepared for consultation, issues raised by the Department, and copies of drafting instructions provided by the Department, to set out what we consider are the key changes and issues in this PIA Update. We have not set out changes which we consider are drafting improvements (e.g. particular phrasing of rules where the substance of the rule has not changed).

2.1 This PIA:

2.1.1 considers how the instruments described in paragraph 1.1 above will meet the principles set out in the Privacy Act, including the APPs;

2.1.2 is intended to help the Department manage identified privacy risks and impacts in respect of the Digital ID System;

2.1.3 considers the safeguards that have been, or should be, put in place to secure personal information from misuse, interference or loss, or from unauthorised access, modification or disclosure; and

2.1.4 may serve to inform the Department, the Australian Parliament, and stakeholders about how privacy has been incorporated into the Digital ID System.

2.2 A glossary of defined terms and acronyms is at Part F [Glossary].

3. Summary of Findings

3.1 The extensive consultation process undertaken by the Department in the development of the Draft Rules and Standards balances privacy considerations with other considerations, including the user experience of the Digital ID System. While we have not identified any significant privacy risks in the Draft Rules and Standards, the Draft Rules and Standards raise the following key privacy risks:

3.1.1 **Risk 1:** There is a potential for increased risk of negative privacy impacts for individuals if the Digital ID Rules do not provide clarity about the circumstances in which information collected under the Digital ID framework is permitted to be handled outside of Australia.

3.1.2 **Risk 2:** There is a risk with the implementation of a 'single blind' model for the identity exchange that individuals will not be made aware, without further active steps being taken, of the potential uses and disclosures of their Digital ID, including when a relying party will be provided details of their identity service provider.

3.2 The recommendations set out in paragraph 4.1 and the privacy best practice recommendations set out in paragraph 4.2 are designed to address the identified risks and further enhance the privacy protections.

4. Recommendations

4.1 This PIA Update makes the following **recommendations**:

Recommendation 1 Data localisation rules

Rationale

Section 77 of the Act provides that the Digital ID Rules may make provision for rules to be made in relation to the holding, storing, handling or transfer of information outside of Australia. Following consultation, the intention is not to include any such rules in the Digital ID Rules on commencement in December 2024, to provide time for further consultation with industry to ensure that users of the Australian Government Digital ID System (**AGDIS**) are not precluded from using 'best-in-class security solutions that may rely on internationally hosted cloud services'.

The above approach removes the previous framework for ensuring oversight of proposed handling of information outside of Australia, and also represents a departure from the general principle in APP 8 (and similar provisions in State/Territory privacy legislation), which is intended to provide additional protections if entities intend on disclosing personal information to a recipient outside of Australia. APP 8 will apply to impose those protections only to the extent that the Privacy Act applies to regulated entities (noting the expanded definition of personal information under the Digital ID Act), but it may not cover all data handled through the Digital ID System.

However, we acknowledge that it is important to also consider the evolution of technology which could further the general principle behind APP 8 to provide additional protections to individuals in Australia and the need to carefully consider and balance options for the Digital ID System. We also acknowledge that the Digital ID Framework will be implemented in a phased approach (by a determination to be made under s 60 of the Act). From a practical perspective, this means that on commencement of the Digital ID Rules in December 2024:

- only government entities will participate in AGDIS;

Recommendation 1 Data localisation rules

- should no rules be made under s 77 of the Act in relation to the holding, storing, handling or transfer of information outside of Australia, APP 8 will continue to apply to Commonwealth government entities in relation to any proposed transfer of personal information overseas (and any equivalent provisions under any State and Territory legislation that apply to State and Territory agencies); and
- under proposed r 3.4 of the Accreditation Rules, entities are required to map their maturity against the ISM Mapping document published by the Australian Cyber Security Centre and these controls apply irrespective of where data is held.

Recommendation

In the context of the Digital ID System being introduced in a phased approach (where other regulatory schemes will protect any personal information that is proposed to be transferred overseas on commencement), but where stakeholders have raised significant concerns about making rules requiring data localisation under the Act, we **recommend** that the Department:

- undertake to further review whether rules under s 77 of the Act are required, and commit to a timeframe for this (for example, this commitment could be made in any announcements and documentation about the phased approach);
- consider any proposed amendments to the Privacy Act prior to finalising the Digital ID Rules, to demonstrate that the final policy position taken in the Digital ID Rules in relation to data localisation takes into account any proposed privacy reforms; and
- in the Explanatory Statement to the Digital ID Rules that are made, or other guidance material on the Digital ID System, explain the security requirements that will apply irrespective of the country in which relevant data is stored, and the data localisation requirements that otherwise apply to regulated entities, to allay potential concerns about any misalignment with the principle behind APP 8.

4.2 This PIA Update makes the following **best practice recommendations**:

Recommendation 2 Sharing of information by the System Administrator

Rationale

Rule 4.5 of the Digital ID Rules provides that the System Administrator may share information it receives with other entities, where it considers it appropriate to do so to 'protect the security, integrity or performance' of the AGDIS. We consider the satisfaction of this specific requirement before the System Administrator can exercise its power to disclose information, to be a privacy enhancing measure. The intention of the information sharing is to enable the System Administrator, Minister, and the Digital ID Regulator, to be able to effectively perform their functions under the Act, including enforcement related functions.

However, we consider that this provision can be further strengthened by requiring the System Administrator to make a written note when it exercises its power under this provision, as a way to demonstrate the seriousness of the data sharing under this provision. This would mirror similar provisions in the Privacy Act where it is important that use of enforcement powers be properly considered and documented.

Recommendation

We **recommend** that the Department consider including in the Digital ID Rules at r 4.5, a requirement that the System Administrator make a written note if it shares information with the Minister, Digital ID Regulator or a participating entity under r 4.5, similar to the requirement at APP 6.5, where the exception in APP 6.2(e) is relied on to disclose personal information in relation to 'enforcement related activities' (as defined under the Privacy Act).

Recommendation 3 Transparency about the operation of the identity exchange

Rationale

The proposed AGDIS Data Standards involve a move to a 'single blind' model for the identity exchange from the current 'double blind' model under the unlegislated Trusted Digital Identity Framework. There is a general perception that such a change will have negative privacy impacts.

However, when the other features of, and protections that have been built into, the Digital ID System are considered, the change in the technical design (to a 'single blind' model) will not increase the risk of data profiling or involve the identity exchange being able to become a central repository of identity data. It will, however, potentially involve some additional limited information about the user being able to be inferred from their choice of identity service provider. It is therefore very important that individuals are informed of the potential downstream uses and disclosures at the time they seek to obtain a digital identity with an identity service provider, including when a participating relying party will be provided details of their identity service provider.

Recommendation

We **recommend** that the Department consider mechanisms that could be employed for individuals to better understand, ideally at the time of seeking a digital identity, the potential uses and disclosures of personal information in the context of the identity exchange.

For example, the Department could seek to impose further requirements on identity service providers and/or participating relying parties, or consider working with the Digital ID Regulator and the Office of the Australian Information Commissioner to develop guidance and standard wording that could be included in relevant notices to be provided to consumers by identity service providers and participating relying parties.

Part B Changes to the Digital ID Rules

5. High Level Overview of the Digital ID Rules

5.1 The Digital ID Rules will be made by the Minister under s 168 of the Act and are disallowable by Parliament. They provide additional requirements for entities participating in the AGDIS.

5.2 The September 2023 version of the Digital ID Rules included draft rules on:

5.2.1 matters relating to the applications to participate in the AGDIS as accredited entities or relying parties;

5.2.2 matters that the Digital ID Regulator must have regard to in determining whether an entity is a 'fit and proper' person;

5.2.3 restrictions on holding and storing system information outside of Australia (except where an exemption is given, including matters that must be established before such an exception is granted by the Digital ID Regulator);

5.2.4 when the interoperability obligations in the Act apply;

5.2.5 the information to be included by entities when reporting:

(a) a cyber security incident; and

(b) a Digital ID fraud incident;

5.2.6 obligations in relation to other matters against which an accredited entity must report, for example, material change in circumstances of the entity; and

5.2.7 obligations in connection with any Digital ID trustmark for the Digital ID System (for example, to use a specified mark, symbol, logo or design in connection with an accredited entity's Digital ID services).

6. Overview of proposed changes to the Digital ID Rules and Privacy Analysis

6.1 Following consultation on the September 2023 version of the Digital ID Rules, the Department refined the drafting of the Digital ID Rules, which it released for further consultation in May 2024. The Department is proposing further changes to the Digital ID Rules. The key changes proposed since the September 2023 version of the Digital ID Rules and their privacy impacts are set out in **Table 1: Proposed Changes to the Digital ID Rules**.

Table 1: Proposed Changes to the Digital ID Rules

Provision	Overview of provision and change	Relevant APP	Discussion on privacy impacts
-	The data localisation rules that appeared in r 10(3) of the September 2023 version of the Rules have been removed.	APP 8 [cross border disclosure]	APP 8 is intended to provide additional protections if entities intend on disclosing personal information to a recipient outside of Australia. The regulation of personal information differs across nations. The disclosure of personal information to an overseas recipient could result in negative consequences for an individual if the same level of privacy protections which apply to their personal information in Australia do not apply to that personal information when it is handled outside of Australia. The Act provides that the Digital ID Rules may make provision for the holding, storing, handling or transfer of information outside Australia by accredited entities within the AGDIS (which is a civil penalty provision) (s 77 of the Act). Any rules so made can be used to place restrictions on holding and storing system information outside of Australia, and to empower the Digital ID Regulator to grant exemptions for any such restrictions. Rule 10 in the September 2023 version of the Rules included draft rules for the purpose of s 77 of the Act. Following consultations, the data localisation rules have been removed from the previous version of the Digital ID Rules. The Consultation Guide provides the following rationale for the removal: *'These would apply in addition to existing legislative obligations to store data onshore. It is not proposed that these would be dealt with on commencement of the Act as further consultation with industry is needed to ensure that these requirements do not preclude users of Digital ID systems from benefiting from best-in-class security solutions that may rely on internationally hosted cloud services.'* In the Original PIA, we recognised that there may be limited circumstances where it may be appropriate for the data localisation rule to not apply, as long as individuals can be confident that their personal information in connection with the Digital ID System will still be appropriately protected. We considered that the proposed r 10 in the September 2023 version of the Digital ID Rules provided a strong framework for the accredited entity (who applies for an exemption) and the Minister (who may grant an exemption) to carefully consider the issues associated with a request to provide personal information to a person outside of Australia.

Provision	Overview of provision and change	Relevant APP	Discussion on privacy impacts
			However, we acknowledge that it is important to also consider the evolution of technology which could further the general principle behind APP 8 to provide additional protections to individuals in Australia and the need to carefully consider and balance options for the Digital ID System. We also acknowledge that the Digital ID Framework will be implemented in a phased approach (by a determination to be made under s 60 of the Act). From a practical perspective, this means on commencement of the Digital ID Rules in December 2024: • only government entities will be able to apply for approval to participate in the Digital ID System (i.e. in the AGDIS); • should no rules be made under s 77 of the Act in relation to the holding, storing, handling or transfer of information outside of Australia, APP 8 will continue to apply to Commonwealth government entities in relation to any proposed transfer of personal information overseas (and any equivalent provisions under any State and Territory legislation that apply to State and Territory agencies); and • under proposed r 3.4 of the Accreditation Rules, entities are required to map their maturity against the ISM Mapping document published by the Australian Cyber Security Centre and these controls apply irrespective of where data is held. Nevertheless, we consider that the following privacy risk arises: ***Privacy Risk 1:*** *There is a potential for increased risk of negative privacy impacts for individuals if the Digital ID Rules do not provide clarity about the circumstances in which information collected under the Digital ID framework is permitted to be handled outside of Australia.* We also note that the *Government Response to the Privacy Act Review Report* indicated some potential changes to APP 8 were being contemplated. In addition, the Privacy and Other Legislation Amendment Bill 2024 contemplates the possibility of regulations being made under the Privacy Act which will enable disclosure of personal information to particular countries outside of Australia without the need to take additional steps to ensure the recipient complies with the APPs.

Provision	Overview of provision and change	Relevant APP	Discussion on privacy impacts
			In our view, any consideration of data localisation for the Digital ID System needs to consider this broader work to ensure a cohesive whole of government approach. In our view, the privacy risk is currently managed given the entities involved but further policy work is required to address data localisation in the context of the Digital ID System before non-government entities participate in the System. Our **Recommendation 1** is intended to assist in addressing these issues.
-	Interoperability rules that appeared in the September 2023 version of the Rules have been removed.	All	The interoperability obligation that appeared in r 11 in the September 2023 version of the Digital ID Rules has been removed to reflect the concerns of stakeholders about limiting consumer choice of accredited digital ID providers. The Consultation Guide provides the following rationale: *'Some stakeholders considered that limiting some Commonwealth services to myGovID (and not commercial digital ID identity service providers) would limit consumer choice of accredited digital ID providers.* *Stakeholders sought clarity regarding the criteria for exemptions to the interoperability obligation. This included clarity as to how a consumer could minimise the need to hold multiple digital IDs. Stakeholders supported the development of publicly available data standards to help inform interoperability requirements to support the digital ID whole of economy ecosystem.* *…The interoperability arrangements are not essential to the effective operation of the system while it remains 'government only' but will be required in future phases of the Australian Government Digital ID System rollout when non-government organisations may join'.* We support the move to having interoperability arrangements included in the Rules when the Digital ID System moves beyond being government only.
Rule 3.3(2)	Requirements for a relying party's application (cyber security and fraud plans) are now included. Refinements to the wording to make clear the following are required to be held (and updated) by a relying party at the time of application: a cyber security plan; a Digital ID fraud management plan; and a written disaster plan.	APP 11 [security]	APP 11 is intended to ensure: that entities take such steps as are reasonable to protect personal information from misuse, interference, and loss, and from unauthorised access, modification, or disclosure; and that they take reasonable steps to destroy the information or to destroy or de-identify personal information that they no longer need. If personal information is not secured and well protected, it could lead to data breaches, resulting in significant harm being caused to affected individuals.

Provision	Overview of provision and change	Relevant APP	Discussion on privacy impacts
			We consider the amendments to this section of the Rules (previously r 7 in the September 2023 version of the Digital ID Rules) are further reasonable steps that entitles can take to protect personal information, which supports the principle behind APP 11.
Rule 4.1 note	Rules now include a note to signpost that an entity is liable for a civil penalty for non-compliance with reportable incidents	APP 1 [transparency] [ensuring compliance]	APP 1 is intended to ensure that entities manage personal information in an open and transparent way and take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs. It is also intended to ensure that individuals dealing with that entity are provided with information about how the entity manages personal information. Section 78 of the Act enables the Digital ID Rules to set out requirements relating to the notification and management of incidents (that is, reportable incidents under the Act). Entities are liable for a civil penalty for failing to meet any such prescribed requirement. Section 78 is regulated by the Privacy Commissioner. We consider this change furthers APP 1. The civil penalty provision signifies the seriousness of reporting and managing incidents as part of the Digital ID System. This proposed change may have the effect of encouraging entities to review their processes and practices (as required under APP 1) to ensure they are equipped to meet the reportable incident requirements.
Rule 4.2(3)(g)	Rule 4.2 sets out when cyber security incidents and digital ID fraud incidents are to be made by entities to the System Administrator (i.e. the Chief Executive Centrelink) and what information is to be included in such notifications. One requirement is that for each individual whose digital ID is affected by an incident, the requirements now require the notice to the System Administration to include when an individual has been informed of the incident, or if they were not so informed, the reasons for this.	APP 1 [transparency] [ensuring compliance]	We consider this requirement furthers APP 1, which requires entities to be transparent. Generally, an entity is expected to notify affected individuals whose Digital ID may have been affected by an incident. However, the provision recognises that there may be circumstances where this may not be appropriate (for example, suspected fraud on the part of the individual). We consider it appropriate for the rules to provide this flexibility. The requirement to provide the entity's reasons for taking a particular position in its notification to the System Administrator furthers the principle of APP 1, by requiring entities to carefully consider (and be able to justify and document) its information handling practices.

Provision	Overview of provision and change	Relevant APP	Discussion on privacy impacts
Rule 4.5	This rule provides that the System Administrator can disclose information it has received (from a participating entity or another means) to other parties (e.g. Minister, Australian Competition and Consumer Commission, another participating entity).	APP 3 [collection] APP 6 [disclosure]	APP 6 is intended to restrict personal information that was collected for one purpose (the primary purpose) from being used or disclosed for another purpose (a secondary purpose), except in specific circumstances (including where the individual has consented to that secondary use or disclosure, or where the use or disclosure is required or authorised by another law). APP 3 sets out the circumstances when entitles can collect personal information. This provision has two intended purposes: • to allow the Minister and Digital ID Regulator to receive information to inform the exercise of powers and functions under the Act (e.g. to revoke approval to participate); and • to enable the System Administrator to coordinate a response to AGDIS incidents and determine which entities are best positioned to assist. We consider including this authorisation in the Rules to enable the System Administrator to share relevant information with other entities (and for those other entities to collect that information) to be reasonably necessary for the System Administrator, the Minister and Digital ID Regulator to effectively undertake their respective functions under the legislative framework. We consider the inclusion of r 4.5(3), which provides that the System Administrator may only give information under this rule if it considers it appropriate to do so to 'protect the security, integrity or performance' of the AGDIS, is a privacy enhancing measure, as it requires the System Administrator to have a strong basis for sharing information with other entities. However, we consider this provision could be further strengthened by the Rules requiring that the System Administrator must make a written note of disclosures when it relies on this provision, similar to the requirement at APP 6.5, where the exception in APP 6.2(e) is relied on to disclose personal information in relation to 'enforcement related activities' (as defined under the Privacy Act). It would be a mechanism by which the System Administrator could record its reasons for believing the information sharing is needed to 'protect the security, integrity or performance of' the AGDIS.

Provision	Overview of provision and change	Relevant APP	Discussion on privacy impacts
			OAIC's APP Guidelines provides at paragraph 6.66 in relation to APP 6.5: '6.66 The APP entity could include the following details in that note: • the date of the use or disclosure • details of the personal information that was used or disclosed • the enforcement body conducting the enforcement related activity • if the entity used the personal information, how the personal information was used by the entity • if the entity disclosed the personal information, who it disclosed the personal information to (this may be the enforcement body or another entity) • the basis for the entity's 'reasonable belief'. This will help the entity assure itself that this exception applies, and it may be a useful reference if the entity later needs to justify its reasonable belief'. See **Recommendation 2**.
Chapter 6	Record-keeping provisions have been amended to include provisions setting out circumstances when prescribed records must not be destroyed or de-identified.	-	The major change in this Chapter since the September 2023 version of the Digital ID Rules is the inclusion of a new provision setting out the circumstances in which records must not be destroyed or de-identified. From a privacy perspective, entities should not retain personal information after it is no longer necessary to do so. The changes set out the limited circumstances where personal information (that is not biometric information) should be retained, with those circumstances relating to anticipated legal proceedings and enforcement actions. In our view, this is reasonable.
Chapter 7	Interim liability arrangement provisions have been removed	-	This change is to facilitate further policy consideration and consultation. We have no comments from a privacy perspective on this.

Part C Changes to the Accreditation Rules

7. High Level Overview of the Accreditation Rules

7.1 The Accreditation Rules will be made by the Minister under s 168 of the Act and are disallowable by Parliament. They will set out the requirements for entities obtaining and maintaining accreditation under the Act.

7.2 The September 2023 version of the Accreditation Rules set out that the key requirements for obtaining and maintaining accreditation include the following:

7.2.1 developing (and submitting to the Digital ID Regulator) a Digital ID privacy policy, a privacy management plan, a cyber security risk assessment, a fraud risk assessment and a PIA (r 2.2);

7.2.2 the PIA submitted must meet the particular requirements provided in the Accreditation Rules, including that it must detail the flow of personal information, include a risk matrix, and be undertaken by an independent person with appropriate expertise, training and qualifications. The entity must respond in writing to the findings in the PIA, and include information about how it will implement the treatments and recommendations of the PIA (r 2.3);

7.2.3 undertaking assurance assessments and systems testing, both on application and on an annual basis[1], including:

(a) a protective security assessment against standards such as ISO 27001, 27002 or the Protective Security Policy Framework;

(b) a fraud assessment that includes a risk matrix and assessment of the ability to respond to emerging risks and threats to the entity's Digital ID data environment;

(c) a usability and accessibility assessment to review accessibility, such as the clear and simple descriptions of the service in multiple accessible formats, and support available to individuals who are unable to use the Digital ID data environment;

(d) penetration testing to evaluate the effectiveness of its security controls by emulating the tools and techniques of likely attackers to exploit security weaknesses;

(e) usability testing to identify any issues in its design, followed by action to mitigate usability issues; and

(f) Web Content Accessibility Guidelines testing against the WCAG Version 2.1 guidelines; and

7.2.4 compliance with the 'data minimisation principle' including only collecting personal information that is reasonably necessary for the accredited entity (or relying party) to provide its services.

[1] See Accreditation Rules, Chapters 3 and 4.

8. Overview of proposed changes to the Accreditation Rules and Privacy Analysis

8.1 Following consultation on the September 2023 version of the Accreditation Rules, the Department refined the drafting of the Accreditation Rules, which it released for further consultation in May 2024. The Department is proposing further changes to the Accreditation Rules. The key changes proposed since the September 2023 version of the Accreditation Rules and their privacy impacts are set out in **Table 2: Proposed Changes to the Accreditation Rules**.

Table 2: Proposed Changes to the Accreditation Rules

Provision	Overview of provision and change	Relevant APP	Discussion on privacy impacts
Rule 4.41	New provision dealing with enduring consent. This rule now provides that the duration of consent given by an individual for any future collection, use or disclosure of the individual's personal information must only be for a maximum of 12 months. Entities with public-facing services must additionally provide individuals with a clear and simple process to withdraw or vary that consent.	APP 3 [collection] APP 6 [use and disclosure]	The proposed amendments are strong privacy enhancing mechanisms. Consent is a crucial aspect of privacy law, as it allows individuals to have control over their personal information. The new provision makes clear that entitles cannot rely on enduring consent, which is in line with privacy best practice. The legislative time frame imposed will ensure equal treatment of individuals across the Digital ID System. The need for a clear and simple process to withdraw and vary consent is also in line with best practice. We also note that the changes are in line with expected changes to the definition of 'consent' under the Privacy Act expected as part of legislation to give effect to the Privacy Act Reforms.
Rule 4.42	This amended provision deals with the data minimisation principle. The September 2023 version of the Accreditation Rules required that an accredited entity must be satisfied that disclosure of personal information to a relying party is reasonably necessary. Changes have been made so that accredited entities that disclose personal information can provide a way for relying parties to minimise the data they collect to provide their services or enable an individual to access their services. Accredited entities will be required to support a technical capability for relying parties and other entities in a Digital ID system to choose to only request some attributes.	APP 3 [collection] APP 6 [disclosure]	The proposed amendments requiring a technical solution to enable relying parties to choose the relevant attributes they require from accredited entities (which will minimise disclosure of personal information by the accredited entity, and collection by the relying party), is a privacy enhancing mechanism. APP 3 is intended to minimise the collection of personal information to that which is reasonably needed by the relevant entity to undertake their particular functions and activities. This is sometimes referred to as the 'data minimisation principle'. Further limitations should apply to the collection of sensitive information (such as prohibiting collection unless the relevant individual has consented to that collection, where the collection is authorised or required by another law, or other specific circumstances apply where it is reasonable to collect that sensitive information). Failure by an accredited entity to adhere to the 'data minimisation principle' could lead to a greater adverse impact on individuals if there was to be a data breach, because of an increased amount of personal information (including sensitive information and information that establishes a person's identity) that may be potentially accessed by a malicious actor.

Provision	Overview of provision and change	Relevant APP	Discussion on privacy impacts
			The amended provision reflects feedback received by the Department about the difficulties with the previous version of the rule, which required the disclosing party to be satisfied that disclosure of personal information to a relying party is reasonably necessary (but did not provide further guidance about the steps that a disclosing party would need to take). As set out in the Consultation Guide: *'This meant that an accredited entity must decide what personal information a relying party requires based on an assessment of the relying party's service, and any justification provided to support the relying party's request for attributes. Most of the feedback received on this issue highlighted the difficulties that would be faced by accredited entities if they were responsible for assessing these risks.'* The amendment works to support the principle behind APP 3 and also supports disclosure in line with APP 6.

Part D Changes to the Accreditation Data Standards

9. High Level Overview of Accreditation Data Standards

9.1 The Accreditation Data Standards are a non-disallowable legislative instrument that support the Accreditation Rules by setting out various technical requirements associated with the accreditation scheme.

9.2 These include:

9.2.1 testing requirements for presentation attack detection technology, biometric matching algorithms, and electronic Identity Document Verification Technology; and

9.2.2 authentication requirements, including the kinds of authenticators, authentication levels bound to a digital ID, and requirements for authenticating an individual to their Digital ID using their biometric information.

10. Overview of proposed changes to the Accreditation Data Standards and Privacy Analysis

10.1 The Department released draft Accreditation Data Standards for public consultation in May 2024. The Department has refined the drafting of the Accreditation Data Standards since then, taking into account stakeholder feedback.

10.2 As the Accreditation Data Standards are quite technical in nature, we have reviewed the standards through a privacy lens to draw out key matters but have not set out in detail all changes that have been made to the Accreditation Data Standards since it was released for public consultation.

10.3 Most of the changes reflect movement of provisions from the Accreditation Rules to the Accreditation Data Standards, as set out in the Consultation Guide:

'Rules relating to authentication management and the testing of biometric technology used in biometric binding solutions, including the testing of a biometric matching algorithm, presentation attack detection technology and eIDVT solutions have been removed from the Accreditation Rules.'

10.4 APP 11 is intended to ensure that: entities take such steps as are reasonable to protect personal information from misuse, interference, and loss, and from unauthorised access, modification, or disclosure; and that they take reasonable steps to destroy the information or to destroy or de-identify personal information that they no longer need.

10.5 We consider the matters set out in paragraph 10.3, now included in the Accreditation Data Standards, to be privacy enhancing measures as they further the principle behind APP 11 based on the commentary included in the Consultation Guide.

Part E AGDIS Data Standards

11. High Level Overview of AGDIS Data Standards

11.1 The *Digital ID (AGDIS) Data Standards 2024* (**AGDIS Data Standards**) outline the technical, data and design requirements for accredited entities and relying parties to participate in the AGDIS. These AGDIS Data Standards apply in addition to the Accreditation Rules, Digital ID Rules and the Accreditation Data Standards.

11.2 The requirements are to ensure that accredited Digital ID service providers and relying parties can communicate securely and reliably.

11.3 The AGIS Data Standards contain three schedules that build on requirements that were used in the Trusted Digital Identity Framework (**TDIF**) (a precursor to the accreditation scheme in the *Digital ID Act 2024*). The AGDIS Data Standards also include definitions and refer to international standards used in the AGDIS Data Standards.

11.4 In summary:

11.4.1 **Schedule 1** presents the AGDIS Onboarding specifications. Outlining the high-level functional requirements for participating accredited entities, this schedule is based on TDIF 06 Functional Onboarding Requirements.

11.4.2 **Schedule 2** outlines the AGDIS OpenID Connect profile and ensures services know how to securely communicate with each other, provide authentication services, and share attributes. This schedule is based on the TDIF 06B OpenID Connect 1.0 profile.

11.4.3 **Schedule 3** describes the AGDIS Attribute Profile. The attribute profile outlines how data being transmitted across the AGDIS must be structured, ensuring participants know how to transmit data and how they will be receiving it.

12. Overview of proposed changes to the AGDIS Data Standards and Privacy Analysis

12.1 On 8 July 2024, Finance conducted a public consultation to gather feedback on the AGDIS Data Standards, which closed on 12 August 2024.

12.2 A variety of stakeholders, including individual contributors, private organisations, and government agencies provided feedback.

12.3 The key themes from the consultation were:

12.3.1 clarity and documentation accuracy;

12.3.2 implementation accuracy and technical corrections;

12.3.3 compliance assurance; and

12.3.4 privacy and data use.

12.4 As the AGDIS Data Standards are quite technical in nature, we have reviewed the standards through a privacy lens to draw out key matters, and have not set out in detail all changes between the TDIF (on which the AGDIS Data Standards build) and the proposed AGDIS Data Standards.

Single blind vs double blind model

12.5 A technical feature of the current unlegislated TDIF is the 'double blind' model for the identity exchange. Under the 'double blind' model, the identity exchange:

12.5.1 does not disclose to identity service providers which relying party services its users are accessing in the AGDIS; and

12.5.2 does not disclose to relying parties which identity service provider a person has used to access one of their service.

12.6 In contrast, the proposed AGDIS Data Standards involves a move to a 'single blind' model for the identity exchange. Under the proposed model, participating Identity Service Providers will continue not to know which participating relying party's services a user is endeavouring to access. However, participating relying parties will be able to ascertain the details of a user's participating identity service provider (i.e. which identity service provider issued the user's Digital ID).

12.7 We make the observation that the perception that such a change will have negative privacy impacts is likely to be heightened, particularly if the overall operation and protections in the AGDIS have not been carefully considered and taken into account.

12.8 The following previous PIAs[2] on the TDIF considered the 'double blind' policy:

12.8.1 Galexia - Initial Privacy Impact Assessment for the Trusted Digital Identity Framework (TDIF) Alpha - 5 December 2016;

12.8.2 Galexia - Second Independent Privacy Impact Assessment (PIA) for the Trusted Digital Identity Framework (TDIF) - September 2018; and

12.8.3 Galexia - 3rd Independent Privacy Impact Assessment (PIA) on the TDIF and related Digital Identity Ecosystem - March 2021.

12.9 Those PIAs found that the 'double blind' model was designed to be a 'privacy positive' feature of the TDIF and was important because it prevents:

12.9.1 the identity exchange from becoming a central repository of identity data – identity service providers do not obtain logs of the services being used by their customers, which ensures identity service providers cannot commercialise this data to profit from the individual, and that the data would be less vulnerable because it is distributed across multiple providers;

12.9.2 a comprehensive trail of how consumers acquired and used their digital identity from being created - any trail could be used to build a 'detailed consumer profile' over time; and

12.9.3 information being used to profile the behaviour of individuals.

12.10 The move to 'single blind' model has been proposed following extensive consultation and review of the current TDIF arrangements. As explained in the *Your Guide to the Digital ID (AGDIS) Data Standards* (the **Guide**), moving to disclosing a user's choice of participating identity service provider to participating relying parties has significant benefits for entities and individuals, including because it:

'…can support improvements to user experience, such as simplifying the process for logging in to a relying party service with a Digital ID. It can also support improved fraud detection, as information about a person's choice of identity provider is information that relying parties can use to better assess the risk of fraud. Stakeholders have also told us that in a future scenario where multiple identity service providers are participating in the AGDIS, access to this would remove one of the barriers currently preventing them from using Digital IDs within

[2] Copies of PIAs can be found at https://www.digitalidsystem.gov.au/what-is-digital-id/privacy-and-security

the AGDIS to meet their 'know your customer' obligations such as those set out in the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) framework.'

12.11 However, as set out in paragraph 12.9 the 'double blind' model was initially implemented for the TDIF to address concerns that entities may potentially profile users from the information they could access through the identity exchange. Australians are concerned with data profiling practices. The *Australian Community Attitudes to Privacy Survey* (August 2023) conducted by the Office of Australian Information Commissioner found that:

'The practices most likely to be considered 'not fair and reasonable' are the online tracking, profiling and targeting of advertising to children (89%) and vulnerable individuals (such as gambling companies targeting gamblers) (88%).'

12.12 Data profiling of consumers has the potential to significantly negatively impact the privacy of individuals, including through discrimination, de-individualisation and stereotyping, particularly in the context of any automated decision making.

12.13 It is, therefore, critical to carefully consider any move to a 'single blind' model and assess the potential privacy impacts on individuals. In assessing the privacy risks and impacts, we have considered the following characteristics of the Digital ID System:

12.13.1 participating identity service providers will continue not to have access to information about the services being used by their customers, which will prevent the participating identity exchange from becoming a central repository of identity data;

12.13.2 it will continue to be difficult (if not impossible) for a comprehensive trail of how consumers acquired and used their digital identity to be created, as the implementation of the 'single blind' technical feature will not capture the relevant information to make this possible;

12.13.3 consistent with the intent of data minimisation, information about an individual's identity service provider can only be disclosed by the identity exchange if a replying party effectively requests provision of that information – so that if this information is not requested, the 'double blind' will remain in place for that relying party; and

12.13.4 the Act includes at s 55 a civil penalty provision which provides that an accredited entity must not use or disclose personal information[3] about an individual that is in the entity's possession or control to offer to (or enable another entity to) supply goods or services; or advertise or promote goods or services (or enable another entity to), which is a strong deterrent for participating relying parties (that are also accredited entities) from using information, including to profile individuals for particular purposes.

12.14 There is a minor residual risk that under the current framework relying parties (which are not accredited entities) may make inferences about users from the user's choice of a particular identity service provider and use that information for marketing and other purposes. We acknowledge the personal information that can be inferred may be relatively limited. Further, where a relying party is an APP entity, the relying party will need to meet the requirements in APP 7 in order to use the inferred personal information for direct marketing purposes which will further reduce the potential for harmful privacy impacts on individuals.

[3] Sub-section 55(2) of the Act includes an exception which provides that information may be disclosed about an individual if it is disclosed to offer the supply of an entity's accredited services, or advertising or promoting of the entity's accredited services or where the individual has consented.

12.15 In our view, considering the Digital ID System features in detail, the change in the technical design of the identity exchange to a 'single blind' model, does not compromise the protection of privacy rights or increase the risk of negative impacts on individuals. The original policy intent (under the TDIF) in relation to minimising the profiling of individuals is maintained while offering other benefits to users (for example, allowing participating relying parties to identify anomalies in the participating identity service provider being used by a user on a particular occasion, and to take steps designed to prevent fraud). The technical measures are now also supported by strong penalty provisions, which further promotes rights to privacy and mitigates against negative impacts.

12.16 However, an important part of promoting the privacy rights of individuals is ensuring that individuals are aware of how their personal information may be used and disclosed. This also provides individuals a level of control over the management of their personal information.

12.17 Entities participating in the AGDIS are required to act transparently (the principle behind APP 1 in the Privacy Act) and are required to provide relevant collection notices at the time they collect personal information (APP 5 in the Privacy Act), however, we consider in the context of the Digital ID, individuals should be informed at the time they seek to obtain a Digital ID with an identity service provider of the potential downstream uses and disclosures, including when a relying party will be provided with details of their identity service provider.

12.18 This raises the following risk:

Privacy Risk 2: There is a risk with the implementation of a 'single blind' model for the identity exchange that individuals will not be made aware, without further active steps being taken, of the potential uses and disclosures of their Digital ID, including when a participating relying party will be provided details of their participating identity service provider.

12.19 Our **Recommendation 3** is a measure to address this.

12.20 We note that publishing the PIAs conducted to date on the TDIF, and now the AGDIS Data Standards, also promotes transparency. At commencement, participating relying parties will be limited to Commonwealth, State and Territory agencies. Information provided to Commonwealth agencies and APP entities will be regulated by Privacy Act including APP 7. Commonwealth agencies will also be regulated by the Australian Government Agencies Privacy Code. In addition, State and Territory agencies will be regulated by their respective privacy legislation.

12.21 Under section 34 of the Act, we note the Minister may enter into an APP-equivalent agreement with a State or Territory department or authority, which may prohibit an entity from collecting, holding, using or disclosing personal information in any way that would breach an Australian Privacy Principle.

Expression of the AGDIS Data Standards

12.22 We note that a number of stakeholders provided feedback on how the standards should be expressed and provided suggested refinement to wording.

12.23 We note that there was at least one stakeholder who opined that the AGDIS Data Standards should incorporate a set of overarching design principles. From a privacy perspective, we make the observation that any standards should be clear. Principles based regulation, while offering flexibility, also increases the risk of departure in practice.

12.24 However, there may be benefit in the Digital ID Data Standards Chair preparing overarching design principles, which could inform the continuing development of the AGDIS Data Standards.

Part F Glossary

Definitions	
Accreditation Data Standards	means the exposure draft of the Digital ID (Accreditation) Data Standards 2024 released on 20 May 2024 available at: https://www.digitalidsystem.gov.au/have-your-say/2024-digital-id-rules-accreditation-rules-and-data-standards, and revised as at 20 September 2024.
Accreditation Rules	means the exposure draft of the Digital ID (Accreditation) Rules 2024 released on 20 May 2024 and available at: https://www.digitalidsystem.gov.au/have-your-say/2024-digital-id-rules-accreditation-rules-and-data-standards, and revised as at 20 September 2024.
accredited entities	means the entities that can provide Digital ID services under the Act, namely identity service providers, attribute service providers, and identity exchange bodies.
Act	means the *Digital ID Act 2024* (Cth) commencing on 1 December 2024 and available at: https://www.legislation.gov.au/C2024A00025/asmade/text.
AGDIS Data Standards	means the Digital ID (AGDIS) Data Standards 2024 available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.digitalidsystem.gov.au/sites/default/files/2024-07/digital_id_agdis_data_standards_2024_1.pdf and as revised on 16 October 2024.
APP Guidelines	means the OAIC's *Australian Privacy Principles guidelines.*
APP, or Australian Privacy Principle	has the meaning given to it in the Privacy Act.
attributes	has the meaning given to it in section 10 of the Act (which is information associated with an individual, including information derived from another attribute).
Bill	means the Digital ID Bill 2023 (Cth).
biometric information	has the same meaning as in section 9 of the Act (which is information about any measurable biological characteristic relating to an individual that could be used to identify the individual or verify the individual's identity and includes biometric templates).
Consultation Guide	means the consultation guide prepared by the Department as part of its May 2024 public consultation process to detail changes to the draft Digital ID Rules and Accreditation Rules since the September 2023 versions.
Department	means the Australian Government Department of Finance.

Definitions	
Digital ID	has the same meaning as in section 9 of the Act (which is a distinct electronic representation of an individual that enables them to be sufficiently distinguished when interacting online with services).
Digital ID Regulator	means the Australian Competition and Consumer Commission, which will act as an independent regulator of the Digital ID system as per section 90 of the Act.
Digital ID Rules	means the exposure draft of the Digital ID Rules 2024 released May 2024 and available at: https://www.digitalidsystem.gov.au/have-your-say/2024-digital-id-rules-accreditation-rules-and-data-standards. and revised as at 20 September 2024.
Digital ID System	means the voluntary accreditation scheme for Digital ID providers and expansion of AGDIS, provided for in the Act.
Draft Rules and Standards	means the framework underpinning the Digital ID System, comprising of the Digital ID Rules, the Accreditation Rules, the Accreditation Data Standards and the AGDIS Data Standards.
OAIC	means the Office of the Australian Information Commissioner, established under the *Australian Information Commissioner Act 2010* (Cth).
Original PIA	means the privacy impact assessment undertaken by Maddocks for the Department in December 2023, with an Addendum added in January 2024.
personal information	depending on the context, has the meaning given in section 6 of the Privacy Act or section 9 of the Act.
PIA	means privacy impact assessment.
PIA Update	means this privacy impact assessment.
Privacy Act	means the *Privacy Act 1988* (Cth).
sensitive information	has the meaning given in section 6 of the Privacy Act.
September 2023 versions	means the exposure drafts of the Digital ID (Accreditation) Rules 2024 and the Digital ID Rules 2024 made available for public consultation in September 2023.
TDIF	means the series of policies which make up the Australian Government's Trusted Digital Identity Framework, and which set out the current requirements that applicants seeking to provide digital identity services need to achieve to meet accreditation.