Maddocks

Department of Finance

Privacy Impact Assessment Update No. 2

Digital ID Framework

Date of analysis – 11 September 2025

Date of finalisation – 10 November 2025

Contents

Part A Executive Summary

1. Introduction

1.1 The Department of Finance (**Department**) is responsible for administering the *Digital ID Act 2024* (Cth) (**Digital ID Act**) and its subordinate legislation, which includes:

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

1.1.2 the *Digital ID (Accreditation) Rules 2024* (Cth) (**Accreditation Rules**).

1.2 Maddocks undertook a privacy impact assessment (**PIA**) in December 2023 (the **Original PIA**), which assessed the privacy impact of:

1.2.1 the exposure draft of the Digital ID Bill 2024 (Cth) and the amendments made to it 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.

1.3 A further addendum to the Original PIA was undertaken in January 2024 (**Amendment PIA**), which supplemented the Original PIA by considering the Digital ID Bill 2024 as further refined after the public consultation processes.

1.4 In November 2024, Maddocks finalised a PIA report which considered, among other things, the privacy impacts of a range of proposed changes to the Digital ID Rules and Accreditation Rules (**PIA Update 1**).

1.5 As part of its 2025 Digital ID subordinate legislation program (**Program**), the Department has now developed the following draft instruments:

1.5.1 the Digital ID Amendment (Redress Framework and Other Measures) Rules 2025 (**Digital ID Amendment Rules**); and

1.5.2 the Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025 (**Accreditation Amendment Rules**),

which include proposed amendments to the Digital ID Rules and the Accreditation Rules, respectively.

1.6 Consistent with the Department's continuing commitment to a 'privacy by design' approach to delivering the Digital ID framework, the Department has engaged Maddocks to undertake a further PIA process (**PIA Update 2**) specifically in relation to the measures described in the Digital ID Amendment Rules and Accreditation Amendment Rules.

2. This PIA Update Process

2.1 Continuing to update previous PIAs as matters change over time is consistent with privacy best practice, as it allows consideration of any new or changed ways of handling personal information as a project evolves, as well as any changes to community expectations of the handling of personal information.

2.2 As discussed in PIA Update 1, PIA processes in respect of proposed new legislation and subordinate legislation 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 update processes such as this one, under which consideration is given to proposed new Australian law, the question then becomes whether that Australian law *should* provide that authorisation. As was done for the Original PIA, Amendment PIA, and PIA Update 1, this PIA Update 2 considers the privacy impacts of the Digital ID framework 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). Although we have considered all APPs for each proposed change, in this report we have only discussed relevant APPs and privacy issues.

2.3 This PIA Update 2 builds on the Original PIA, Amendment PIA and PIA Update 1, but focuses solely on the proposed changes contained in the Digital ID Amendment Rules and the Accreditation Amendment Rules. It does not seek to reconsider or reassess issues that were discussed, or recommendations that were made, in these PIAs if those issues are not relevant to the changes now being proposed.

2.4 We have conducted our analysis of the proposed changes based on the drafts of the Digital ID Amendment Rules and Accreditation Amendment Rules as at 3 November 2025, and the associated draft Explanatory Statements. We have not considered any further refinement of those drafts after this date. We have described the key changes which we believe have associated privacy issues in this report, but have not described every change in detail.

2.5 Our analysis is based upon the provisions of the Privacy Act, and associated case law and guidance material, as in force at the date of analysis on the cover page of this PIA Update 2 report. This includes the commenced reforms introduced by the *Privacy and Other Legislation Amendment Act 2024* (Cth) (**POLA Act**). While we have endeavoured to take into account proposed reforms that were not introduced by the POLA Act, in particular those further reforms discussed in the *Privacy Act Review Report*[1] released by the Attorney General's Department and the Australian Government's response to the *Privacy Act Review Report,*[2] it may be advisable for the Department to seek further advice about the privacy implications of those reforms should they be implemented.

2.6 This PIA Update 2:

2.6.1 considers any privacy impacts of relevant proposed changes by considering them against the underlying principles of the Privacy Act, including the APPs;

2.6.2 is intended to help the Department manage identified privacy risks and impacts in respect of the Digital ID Amendment Rules and Accreditation Amendment Rules, including by implementing feedback received from stakeholders during consultation conducted by the Department in relation to the Program;

2.6.3 makes recommendations designed to address identified potential privacy risks, or areas where further improvement could be considered; and

2.6.4 may serve to inform the Department, the Australian Parliament, and stakeholders about how privacy continues to be incorporated into the ongoing design Digital ID framework.

---

[1] https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.
[2] https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report#:~:text=In%20its%20response%20to%20the,to%20best%20protect%20this%20information.

2.7 A glossary of defined terms and acronyms is at **Part D [Glossary]**.

3. Summary of Findings

3.1 In relation to the changes proposed by the Digital ID Amendment Rules, we consider that the proposed changes will generally support the existing 'privacy-by-design' approach to the overall Digital ID framework in the Digital ID Act, Digital ID Rules, the Accreditation Rules, and the other subordinate legislation.

3.1.1 In our view, implementing the **Redress Framework** within the Digital ID Amendment Rules will be an important step towards supporting individuals' ability to efficiently deal with, and obtain assistance in relation to, cyber security and/or Digital ID fraud incidents (**Incidents**) occurring in relation to accredited services provided within the Australian Government Digital ID System (**AGDIS**). In particular, we consider that:

(a) implementation of a framework for notification of Incidents by certain Attribute Service Providers (**ASP**) and Identity Service Providers (**ISP**) (together, **Providers**) will further an affected individual's ability to take any steps that would minimise potential harms to them. However, we consider that the Department should consider whether there is a potential need for additional guidance about the matters about which a Provider will need to be satisfied before it will not be required to notify affected individuals;

(b) the additional requirements for Providers to develop and publish policies relating to their incident and complaints management processes will allow further openness and transparency for individuals with a Digital ID, and should also facilitate Providers being able to respond more quickly in the event of an Incident; and

(c) mandatory referral of technical issues to the **System Administrator** by Providers in certain circumstances, will further promote trust in the AGDIS by providing individuals with greater confidence that appropriate redress will be provided, and is likely to promote accountability of entities through referral to the System Administrator.

3.1.2 We also consider that reducing the mandatory matters that the Digital ID Regulator must consider when reviewing an application for participation in the AGDIS made by government entities following a 'machinery of government' (**MOG**) change, will facilitate individuals continuing to be able to use their Digital ID, without additional adverse impacts on their privacy.

3.1.3 We have not identified any adverse privacy impacts for individuals associated with the proposed changes to the use of the Digital ID Accreditation Trustmark (**Trustmark**) by the Digital ID Data Standards Chair (**Data Standards Chair**).

3.1.4 Similarly, we have not identified any adverse privacy impacts for individuals associated with the changes which would give the System Administrator the ability to direct an entity that has interacted with a Digital ID affected by an Incident, to conduct an investigation into the Incident.

3.2 In relation to the proposed changes to the Accreditation Rules, we again do not consider that the majority of these changes are likely to involve significant adverse impacts on the privacy of individuals using their Digital ID.

3.2.1 We consider that the proposed changes in relation to the incorporation of the Protective Security Policy Framework (**PSPF**) by reference to the relevant requirements, rather than by replication of the requirements within the Accreditation Rules, is a privacy-enhancing measure because it will ensure that the applicable PSPF controls will remain in-step with any updates to the PSPF and so remain fit-for-purpose. We have also not identified any adverse privacy impacts associated with Non-Corporate Commonwealth Entities (**NCCEs**) being required to comply with the applicable PSPF controls.

3.2.2 However, these changes do highlight an existing risk that the transition periods for compliance with future changes to the PSPF (or other applicable security frameworks incorporated by reference) may mean that Providers do not take immediate actions necessary to address any new security threat that rapidly develops, and which triggers an urgent change to the PSPF (or other applicable security framework), as such action may not be taken until the end of the applicable transition period. While this raises the potential risk that individuals may be exposed to increased security risks in relation to their Digital IDs during this time, we appreciate that the Digital ID Regulator has existing broad directions powers under the Digital ID Act that could be used to direct Providers to comply with urgent changes to the PSPF (or other applicable security framework) within a shorter time period.

3.2.3 While we understand the need for a distinction to be made between the period in which consent for handling of their personal information should be re-obtained by ASPs from individuals who are using their Digital ID in their personal capacity, and those who are using it to undertake transactions for a business, we are concerned that the proposed period of 7 years may be considered too long, and that a shorter period may be more appropriate.

3.2.4 We have not identified any significant adverse privacy impacts for individuals associated with the proposed changes to provide transitioned accredited entities with an additional 12 months within which to comply with particular requirements for individuals to suspend and resume use of their Digital ID, given other existing rights of those individuals to otherwise effectively control use of their Digital ID.

3.3 The risks we have identified are discussed further in **Part B [Changes to the Digital ID Rules]** and **Part C [Changes to the Accreditation Rules]**. The recommendations set out in paragraph 4 below are designed to address these identified risks and further enhance privacy protections, and / or further strengthen compliance with privacy best practice and privacy-by-design principles.

4. Recommendations

4.1 This PIA Update 2 makes the following recommendations in relation to the Digital ID Amendment Rules and Accreditation Amendment Rules:

Recommendation 1	Digital ID Amendment Rules – Redress Framework

Rationale

It is important that individuals are, when appropriate, notified of Incidents, as a failure to do so may mean that an individual cannot effectively take steps to minimise the harm caused to them by the Incident.

Recommendation 1	Digital ID Amendment Rules – Redress Framework

The Provider will be responsible for determining whether or not notification of an Incident to an individual will, or could reasonably be expected to, have 'a material effect on the operation of the AGDIS', but we anticipate that it may perhaps be difficult for Providers to understand and apply this test in practice.

Recommendation

We recommend that the Department consider whether it would be necessary or desirable to provide further guidance or directions to Providers about the interpretation and application of the matters about which a Provider must be satisfied before they are not required to notify individuals of an Incident, and if so, how best to do so.

Recommendation 2	Accreditation Amendment Rules – Duration of consent for business users

Rationale

ASPs will only need to seek consent from individuals using their Digital ID on behalf of a business every 7 years. This period seems very long in the context of an individual's engagement with a business, given an individual's relationship with a business is very likely to change over the course of that period. The measure assumes that 7 years is an appropriate period for a consent given at the start of that period to remain current and specific, and effectively shifts responsibility from the ASP (to actively seek consent) to the relevant individual / business (to withdraw their consent, or update the attribute).

We do appreciate that:

- an individual using a Digital ID on behalf of a business may have specified a period of time for which their consent will continue that is less than 7 years (for example, if an ASP provided an option for an individual to specify a lesser period at the time of seeking consent, this would mean that the consent would only apply for that lesser period under Rule 4.41(3)(a));
- an individual can withdraw or vary their consent at any time (Rule 4.41(2)), resulting in it continuing for a period of less than 7 years (including because of the operation of Rule 4.41(b)); and
- when using a Digital ID to act on behalf of a business, the only information shared about the individual is their full name, contact details, and the relevant attribute (e.g. the name of the business and the nature of their authority to act on behalf of the relevant business).

We understand that stakeholders consulted by the Department provided differing feedback about this change, with most indicating support for the change but others expressing reservations.

Recommendation

We recommend that the Department explore whether a shorter period than 7 years should be specified as the relevant period, and / or potentially explain the policy reasons for selecting the applicable period for the duration of the relevant consent.

4.2 We understand that the Department will separately document its responses to the above recommendations.

Part B Changes to the Digital ID Rules

5. High Level Overview of Changes to the Digital ID Rules

5.1 The Digital ID Amendment Rules will, if passed, amend the Digital ID Rules to:

5.1.1 address cyber Incidents that occur, or are reasonably suspected to have occurred, in relation to the accredited services provided by accredited entities within the AGDIS, by providing for a Redress Framework applicable to certain Providers;

5.1.2 in relation to MOG changes which transfer functions for the provision of services within the AGDIS from a relying party approved for participation in the AGDIS (**transferring entity**) to another entity (**receiving entity**), provide a streamlined process for the application of receiving entities to provide those services;

5.1.3 include the Data Standards Chair as an authorised entity in relation to the use or display of the Trustmark; and

5.1.4 provide a framework for the System Administrator to direct entities to undertake investigation of Incidents in certain circumstances, and provide procedures for entities to conduct investigations directed by the System Administrator.

5.2 Set out below is further information about each of these proposed amendments to the Accreditation Rules and our corresponding privacy analysis.

6. Introduction of the Redress Framework

The Changes

6.1 The Digital ID Act requires that, within 12 months of the commencement of the Digital ID Act,[3] the Digital ID Rules must provide for a redress framework for incidents that occur in relation to services provided by approved entities within the AGDIS, and specifies the mandatory matters to be dealt with in that framework.[4] Relevantly, the Digital ID Amendment Rules will:

6.1.1 establish a Redress Framework that applies to Providers that are:

(a) a participating entity;

(b) an entity whose approval to participate is suspended; or

(c) an entity whose approval to participate has been revoked;

6.1.2 provide that in the event of an Incident in relation to an accredited service, the Provider of that service must make reasonable attempts to notify each individual affected by the Incident, unless it is satisfied that:

(a) there is a likelihood of the individual suffering an adverse outcome as a result of the Provider attempting to notify the individual of the Incident; or

[3] Digital ID Act, s 88(1).

[4] Digital ID Act, s 88(2).

(b) notifying the individual will, or could reasonably be expected to, have a material effect on the operation of the AGDIS;[5]

6.1.3 provide for mandatory referral, as soon as reasonably practicable after becoming aware (or if the Provider becomes aware because of a complaint made by an individual, within 28 days after receipt of the complaint), by a Provider of an unresolved technical issue to the System Administrator if:

(a) the issue relates to a cyber security incident or Digital ID fraud incident which has occurred, or is reasonably suspected of having occurred, in relation to an accredited service provided by a Provider (i.e. it is an Incident);

(b) the Incident is within the control of the Provider or another Provider;

(c) as a result of the Incident, an individual is unable to use their Digital ID;

(d) the Provider is reasonably satisfied that the Incident cannot be resolved without referring it to the System Administrator; and

(e) the Provider has complied with Rule 4A.5 (if applicable), which will require Providers to:

(i) direct the individual to any relevant public resources, including the information published by the Provider on the resolution of Incidents and the Provider's complaints processes (see paragraph 6.1.5 below); and

(ii) if the individual is unable to use their Digital ID due to a technical issue with the Provider's service that is within the control of another Provider, provide reasonable assistance to help the individual identify that other entity and its contact details;

6.1.4 provide that the System Administrator may recommend a resolution to an Incident referred to it by a Provider, with resolutions available to it for recommendation including that the Provider provide an explanation of the circumstances or an apology to the affected Individual;[6] and

6.1.5 provide that Providers that are participants in the AGDIS (i.e. Providers whose approval to participate has not been suspended or revoked) must develop and publish policies addressing:

(a) the identification, management and resolution of Incidents; and

(b) the process by which an individual can make a complaint to the Provider, its procedures for dealing with complaints, and timeframes for its resolution of complaints.[7]

[5] Rule 4A.2(2).

[6] Rule 4A.4.

[7] Part 5 – Policies relating to incidents and complaints.

Discussion of potential privacy impacts

6.2 The proposed Redress Framework contains a number of amendments that represent new privacy and other protections for individuals, rather than matters that would negatively impact on their privacy rights. In particular:

6.2.1 It is privacy-enhancing that Providers will be required to notify the System Administrator of any unresolved technical issues relating to an Incident in particular circumstances, given that this will further assist the System Administrator to take steps to ensure that the AGDIS is operating in a secure manner (consistent with the principles behind APP 11.1). Although this process is likely to involve disclosure of an individual's personal information (in their Digital ID) to the System Administrator, such notification already occurs under the other notification requirements under the Digital ID Rules, and we consider that this authorisation by law is reasonable and proportional given the benefits to the individual that flow from it.

6.2.2 It is also positive that the System Administrator will be able to recommend a course of action to resolve an Incident referred by a Provider, including by recommending that a Provider provide an explanation of the circumstances or an apology to the affected individual. We note that there is no requirement for a Provider to implement a recommendation, but this measure at least has the potential to further enhance the security of the solution (consistent with APP 11.1), and to further assist to ensure that there is openness and transparency for individuals in relation to their Digital IDs (consistent with the principles behind APP 1). We also note that the changes do not affect the compliance powers of the Digital ID Regulator, or limit the other powers of the System Administrator.

6.2.3 Providers will be required to develop and publish policies in relation to the identification, management and resolution of Incidents, and their complaints processes. This should facilitate Providers being able to respond more quickly in the event of an Incident, and also assist to ensure that there is a greater level of openness and transparency for individuals in relation to the operation of their Digital IDs within the AGDIS, consistent with the principles behind APP 1. We observe that such policies should reference the potential disclosure of an individual's information in or about their Digital ID to the System Administrator, as proposed by the measures discussed in paragraph 6.2.1.

6.2.4 The Redress Framework also contains measures by which individuals must be provided with information, support and assistance, by being directed to any relevant public resources, which may be relevant to resolution of an Incident or complaint; and provided with reasonable assistance to help the individual in certain circumstances. Again, we consider that these measures will help individuals better understand (and effectively take steps to control) the handling of their personal information associated with their Digital IDs.

6.3 Individuals may experience significant harms (e.g. identity fraud, distress) if an Incident occurs, and some of these harms could be mitigated or minimised if an individual is notified of the Incident and can proactively respond to any risks. We therefore consider that the requirement in the Redress Framework for Providers to make reasonable attempts to notify individuals impacted by an Incident, unless they are satisfied that one of the two exceptions discussed in paragraph 6.1.2 applies, is a privacy-enhancing measure, particularly in circumstances where this requirement will also apply to Providers whose approval to participate is suspended or has been revoked.

6.4 We note that the current drafting does not prescribe a maximum time by which a Provider, after becoming aware of an Incident, must have determined whether to notify the relevant individual of an Incident (and must have so notified that individual if this is the outcome of the determination).

6.5 The Explanatory Statement explains:

> *1.43 The requirement to make reasonable attempts to notify an affected individual under rule 4A.2 does not prescribe a specific timeframe within which to do so. This provides for circumstances where it may not be appropriate to notify the individual immediately or at all.*

6.6 While we agree that there may be circumstances in which it may not be appropriate to notify the individual immediately, we are concerned that the failure to specify *any* timeframes means that Providers may therefore take a longer time than is necessary to make a decision, or to then notify relevant individuals. This could result in delays which may impact the effectiveness of the notification regime in preventing harms to individuals.

6.7 However, there is an existing obligation on Providers (see Rule 4.2) to notify the System Administrator of any Incident *'as soon as practicable after, and in any event no later than 1 business day after, the entity becomes aware that an incident has occurred or reasonably suspects an incident has occurred*', and that this notification must explain, for each individual whose Digital ID is affected by the Incident:

6.7.1 if the individual has been informed of the Incident – when the individual was informed of the Incident; or

6.7.2 if the individual has not been informed of the Incident – why the individual has not been informed of the Incident.

6.8 That is, it is privacy enhancing that there is an existing mechanism via which the System Administrator will be aware as to whether individuals have been notified of an Incident and could, if necessary, engage with the Provider about any failure to issue a notification.

6.9 Finally, we support the proposal in the Digital ID Amendment Rules to specify matters which must be taken into account by Providers when determining whether an exception to notifying an individual about an Incident applies.

6.10 However, we are concerned that there may be some uncertainty about the circumstances in which notifying an individual will, or could reasonably be expected to, have a material effect on the operation of the AGDIS. We note that the Explanatory Statement explains that:

> *1.42 Note 2 informs readers that the term 'material effect' is defined in subrule 1.4(2) of the Digital ID Rules. In this context, a material effect on the AGDIS could be triggered if the notification of the individual could exacerbate the incident to a magnitude that would cause the degradation or loss of functionality within the AGDIS, or limit the ability of an entity to participate in the AGDIS. For example, this could occur if the notification alerted the malicious actor and resulted in a cyber security incident or digital ID fraud incident with greater impact.*

6.11 We consider that these examples represent ones where it seems appropriate for notification to be withheld, but note that this guidance is not exhaustive. We therefore recommend that the Department should give consideration to how best to provide any other guidance to Providers about this matter (**Recommendation 1**).

7. Streamlined Applications For Relying Parties following MOG Changes

The Changes

7.1 Relying parties must apply under section 61 of the Digital ID Act to the Digital ID Regulator for approval to participate in the AGDIS. The Digital ID Regulator can approve applications and may impose conditions, including conditions relating to the services that the relying party may provide, on an approval. An approval cannot be transferred or extended to another entity. This means that currently, if a government entity anticipates that the service(s) it provides within the AGDIS will be transferred as a result of a MOG change, a new application must be submitted by the receiving entity.

7.2 To minimise disruption to services within the AGDIS as a result of MOG changes, the Digital ID Amendment Rules propose to reduce the mandatory matters that the Digital ID Regulator must consider when reviewing an application made by particular government entities.

Discussion of potential privacy impacts

7.3 We have not identified any relevant privacy risks associated with these changes.

7.4 The matters that the Digital ID Regulator will no longer need to consider for a streamlined application by the receiving entity should not have changed as a result of the MOG change, and should not impact the Digital ID Regulator's decision about whether or not the receiving entity is suitable to be approved. The changes should ensure continuity of service for individuals. Once approved, the receiving entity will need to comply with the full range of obligations for a relying party in the AGDIS, irrespective of the streamlined application.

8. Trustmarks

The Changes

8.1 The Digital ID Act establishes the use and regulation of Trustmarks, which are marks, symbols, logos or designs which may be used by accredited entities and participating relying parties as a visual indicator of accreditation or approval, or by authorised entities as specified in the Digital ID Rules. There is currently only one Trustmark specified in Schedule 1 to the Digital ID Rules.

8.2 The Digital ID Amendment Rules will add the Data Standards Chair as an entity authorised to use or display the Trustmark in connection with its statutory functions, which will have the effect of enabling the Data Standards Chair to use or display the Trustmark as part of materials which it may develop to support the performance of its statutory functions.

Discussion of potential privacy impacts

8.3 We have not identified any adverse privacy risks for individuals associated with this proposed change.

9. Further Investigation of Reportable Incidents

The Changes

9.1 Amongst other things, Rule 4.2 imposes obligations on Providers to notify the System Administrator of Incidents. The Digital ID Amendment Rules will:

9.1.1 provide that if the System Administrator is notified of an Incident, it may direct an entity which has interacted with a Digital ID affected by the Incident to conduct an investigation into the Incident;[8]

9.1.2 require that if the System Administrator directs an entity to conduct an investigation, that entity must begin the investigation as soon as reasonably practicable and must provide the System Administrator with a summary of the findings of the investigation as soon as reasonably practicable after the investigation is complete;[9] and

9.1.3 provide that if an investigation conducted by an entity exceeds a period of 28 days, that entity must provide the System Administrator with updates on the progress of the investigation immediately after the 28 days and at least once every 28 days until the investigation is complete.

Discussion of potential privacy impacts

9.2 We consider that it is appropriate that the System Administrator will have broad powers to direct entities to undertake timely investigations into Incidents. This will assist in ensuring the security of the AGDIS, by ensuring that issues that may affect the security of the system are identified and resolved.

9.3 This will support the existing Rule 4.2(3)(e) of the Digital ID Rules, which already provides that a Provider making a mandatory notification to the System Administrator about an Incident must provide a broad range of information about the Incident. If the System Administrator considers that this information is insufficient (noting that it is a relatively comprehensive list), it can direct further investigation into the Incident.

9.4 We have not identified any privacy concerns associated with these changes.

[8] Rule 4.2(7).

[9] Rule 4.2(8).

Part C Changes to the Accreditation Rules

10. High Level Overview of Changes to the Accreditation Rules

10.1 The Accreditation Amendment Rules will, if passed, amend the Accreditation Rules to:

10.1.1 revise the compliance model for the PSPF;

10.1.2 provide an alternative period for the expiry of express consent given by an individual in relation to their use of an ASP's accredited services for or on behalf of a business; and

10.1.3 extend the time within which the requirements under Rule 5.7 and Rule 5.9(2) will apply to transitioned accredited entities.

10.2 Set out below is further information about each of these proposed amendments to the Accreditation Rules and our corresponding privacy analysis.

11. PSPF

The Changes

11.1 The PSPF sets out the protective security policy of the Australian Government and prescribes the protective security requirements for specified Australian Government entities. Select controls of the PSPF are currently incorporated in the Accreditation Rules as a protective security framework available for implementation under Rule 4.2, which requires that accredited entities comply with one of the specified frameworks to maintain accreditation. The Accreditation Amendment Rules will:

11.1.1 incorporate the PSPF by reference to requirements in the PSPF instead of replication in the Accreditation Rules;[10]

11.1.2 mandate that if an accredited entity is an NCCE, as defined in the PGPA Act, it must comply with the relevant PSPF controls in respect of its accredited services and DI data environment;[11]

11.1.3 provide a 3-month transition period for entities to comply with any changes to the PSPF that occur after the commencement of the Accreditation Amendment Rules, in contrast to the 12-month period which will remain applicable to changes to other incorporated instruments;[12] and

11.1.4 require that accredited entities which are not NCCEs must comply with either all of the controls specified in ISO/IEC 27001 or the controls of an alternative framework which includes all the same kinds of controls specified in ISO/IEC 27001.

[10] Rule 4.3.

[11] Rule 4.2(2). Note that 'DI data environment' has the same meaning as in the Accreditation Rules

[12] Rule 1.7(2).

Discussion of potential privacy impacts

11.2 Compliance with the PSPF or another applicable security framework is an important consideration in ensuring a Provider will be able to appropriately protect the personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure (which is consistent with the principles behind APP 11.1).

11.3 In particular, we consider the incorporation of the PSPF by reference to the relevant requirements, rather than by replication of the details of the requirements within the Accreditation Rules, is a privacy-enhancing measure because it will ensure that the applicable PSPF controls will remain in-step with any updates to the PSPF and so remain fit-for-purpose. Without this measure, there may be delays in updating the applicable parts of the Accreditation Rules to reflect changes to the PSPF. We also have not identified any adverse privacy impacts associated with NCCEs being required to comply with the applicable PSPF controls. We consider these measures are therefore additional reasonable steps to ensure that Providers will meet requirements that ensure personal information will be appropriately protected against misuse, interference and loss, and from unauthorised access, modification or disclosure (consistent with the principles behind APP 11.1).

11.4 We also acknowledge that, for practical reasons, there is likely to be a need for a transition period, in which relevant Providers can change their systems, processes and policies in order to comply with any changes to the PSPF that occur after the commencement of the Accreditation Amendment Rules. We are conscious that the Accreditation Amendment Rules specify a shorter period than the existing transitional period for incorporated instruments of 12 months (which will continue to apply for other applicable security frameworks).

11.5 However, this change highlights a concern that there may be a situation in future in which a new security threat rapidly develops requiring urgent attention by Providers in order to avoid a critical security issue. Assuming that such a threat results in an urgent change to the PSPF (or other applicable security framework), relevant Providers would not be required to take action until the end of the transition period.

11.6 We appreciate that entities participating in the Digital ID framework are likely to have other privacy obligations (e.g. under APP 11.1), obligations as an NCCE (for example, under the PSPF), or other incentives to address such risks within their IT environment.

11.7 We also appreciate that section 128(1) of the Digital ID Act provides that the Digital ID Regulator may give a direction to a Provider *'if the Digital ID Regulator considers it necessary to do so to protect the integrity or performance of the Australian Government Digital ID System'*. It will be important that if a new security threat rapidly develops and requires urgent attention by Providers in order to avoid a critical security issue, the Digital ID Regulator considers issuing a direction under section 128(1) of the Digital ID Act to Providers.

12. Duration of Express Consent

The Changes

12.1 An accredited entity cannot disclose certain attributes of an individual to a relying party when verifying that individual's identity, Digital ID, or information about them, without the express consent of that individual.[13] Currently, a relying party can rely upon consent given to accredited entities provided that the consent has not been withdrawn or expired. The duration of express consent provided by an individual to an accredited entity for the future collection, use or disclosure of that individual's personal information is prescribed in Rule 4.41(3), with consent expiring at the earliest of the periods described in that provision.[14]

12.2 The Accreditation Amendment Rules will mean that if, in respect of a service provided by an ASP, an individual declares in their consent that their use of that service is for or on behalf of a business (including a business carried on by that individual), the consent will expire 7 years after the consent was initially given (unless an earlier period under Rule 4.41(3) applies).

Discussion of potential privacy impacts

12.3 Consent is a crucial aspect of privacy law, as it allows individuals to have control over their personal information. The *Australian Privacy Principles guidelines*, issued by the Office of the Australian Information Commissioner (**OAIC**), emphasise that the key elements of consent are that the individual is adequately informed before giving consent, the individual gives consent voluntarily, the consent is current and specific, and the individual has the capacity to understand and communicate their consent. We note that consent given by an individual for the future collection, use or disclosure of to an accredited entity will expire at the earliest of the periods specified in Rule 4.41(3) and provisions for withdrawal of consent will remain unchanged.

12.4 The current 12 month expiry period for express consent for individuals reflects a privacy-protective approach consistent with OAIC guidance, which provide that express consent should not be enduring.

12.5 We consider that it is appropriate that the maximum 12 month period continues to be appropriate in the context of personal use of Digital IDs, in that this will require regular renewal to ensure that consent remains valid and informed.

12.6 In relation to the maximum 7 year period for individuals wishing to use their Digital ID to undertake interactions with relying parties in a business context that requires confirmation of their attributes (authority to act for that business), we understand that the proposed changes are intended to reflect a balance between continuing to protect privacy, and removing unnecessary administrative and regulatory burden for such individuals, which may impact business productivity and services. We also appreciate that:

12.6.1 an individual using a Digital ID on behalf of a business may have specified a period of time for which their consent will continue that is less than 7 years (for example, if an ASP provided an option for an individual to specify a lesser period at the time of seeking consent, this would mean that the consent would only apply for that lesser period under Rule 4.41(3)(a));

[13] Digital ID Act, s 45.

[14] Rule 4.41(3).

12.6.2 an individual can withdraw or vary their consent at any time (Rule 4.41(2), resulting in it continuing for a period of less than 7 years (including because of the operation of Rule 4.41(b)); and

12.6.3 when using a Digital ID to act on behalf of a business, the only information shared about the individual is their full name, contact details, and the relevant attribute (e.g. the nature of their authority to act on behalf of the relevant business).

12.7 While we understand this reasoning, individuals using their Digital ID on behalf of a business still have privacy rights. A 7 year period seems a very long period in the context of an individual's engagement with a business – over the course of that period an individual's relationship with a particular business may be very likely to change, and it may not be appropriate to assume that a consent given 7 years ago remains valid for the entire period (in other words, the measure assumes that this period is appropriate for the consent to remain current and specific, which are requirements for a valid consent). We are also concerned that during this length of time an individual may no longer be affiliated with a business, meaning that inaccurate or out of date personal information will be used if neither the individual or the business takes the necessary steps to update their consent, attributes or authorities. Such a lengthy period may not align with community expectations around data control and accountability, especially as the measure effectively shifts the responsibility from the ASP (to actively seek consent) to the individual (to withdraw their consent, or update their attribute).

12.8 However, some of these risks could be mitigated by ensuring that individuals are regularly reminded that they have provided the relevant consent, which will assist to prompt individuals to withdraw their consent or update their attributes, if necessary.

12.9 Accordingly, we recommend that the Department further consider whether a shorter period than 7 years should be specified as the relevant period, and potentially explain the policy reasons for selecting this period, and otherwise consider whether individuals should be provided with reminders about their consent (**Recommendation 2**).

13. Suspension and Resumption

The Changes

13.1 Rule 5.7 requires ISPs to fulfil an individual's request to temporarily suspend the use of their Digital ID as soon as practicable after confirming the legitimacy of the request, and to notify the individual of the suspension and the process to resume the use of their Digital ID.

13.2 Rule 5.9(2) prescribes the steps that an ISP must take to resume the use of a Digital ID suspended under Rule 5.7, including that the ISP must ensure that the individual completes identity proofing at the same identity proofing level as prior to suspension.

13.3 The Accreditation Amendment Rules will amend the Accreditation Rules to provide transitioned accredited entities with an additional 12 months to comply with these requirements, with a specified date of 30 November 2026 to achieve compliance.[15]

[15] Rule 1.8(1A).

Discussion of potential privacy impacts

13.4 While this amendment will further delay an individual's right to suspend and resume use of their Digital ID by transitioned accredited entities, we note that individuals will continue to be able to achieve a similar level of control by cancelling their Digital ID and creating a new Digital ID.

13.5 Accordingly, we do not consider that these proposed amendments raise significant privacy risks.

Part D Glossary

Definitions	
Accreditation Amendment Rules	means the Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025.
Accreditation Rules	means the *Digital ID (Accreditation) Rules 2024* (Cth).
AGDIS	stands for Australian Government Digital ID System.
Amendment PIA	means the Addendum to the Original PIA, undertaken in January 2024.
APP, or Australian Privacy Principle	has the meaning given to it in the Privacy Act.
ASP	stands for Attribute Service Provider, which has the same meaning as 'accredited attribute service provider' in the Digital ID Act.
Data Standards Chair	means the Digital ID Data Standards Chair.
Department	means the Australian Government's Department of Finance, which has responsibility for administering the Digital ID Act and its subordinate legislation, and for conducting the Program.
Digital ID	has the same meaning as in the Digital ID Act.
Digital ID Act	means the *Digital ID Act 2024* (Cth).
Digital ID Amendment Rules	means the Digital ID Amendment (Redress Framework and Other Measures) Rules 2025.
Digital ID Regulator	means the Australian Competition and Consumer Commission.
Digital ID Rules	means the *Digital ID Rules 2024* (Cth).
Incidents	means cyber security and Digital ID fraud incidents.
ISP	stands for Identity Service Provider, which has the same meaning as in the Digital ID Act.
MOG	stands for machinery of government.
NCCE	stands for Non-Corporate Commonwealth Entity, which has the same meaning as in the PGPA Act.
OAIC	means the Office of the Australian Information Commissioner.
Original PIA	means the PIA undertaken in December 2023.
personal information	has the meaning given in section 6 of the Privacy Act.
PGPA Act	means the *Public Governance, Performance and Accountability Act 2013* (Cth).

Definitions	
PIA	stands for 'privacy impact assessment'.
PIA Update 1	means the PIA report finalised in November 2024 in relation to the privacy impacts of a range of proposed changes to the Digital ID Rules and Accreditation Rules.
PIA Update 2	means this PIA, undertaken in relation to the measures described in the Digital ID Amendment Rules and Accreditation Amendment Rules.
POLA Act	means the *Privacy and Other Legislation Amendment Act 2024* (Cth).
Privacy Act	means the *Privacy Act 1988* (Cth).
Program	means the Department's 2025 Digital ID subordinate legislation program, under which the Department has developed the Digital ID Amendment Rules and the Accreditation Amendment Rules.
Providers	means ASPs and ISPs.
PSPF	stands for Protective Security Policy Framework.
receiving entity	if the Digital ID Amendment Rules are passed, means, in the context of streamlining applications, an entity which will inherit functions in relation to the provision of services with the AGDIS from a transferring entity as part of a MOG change.
Redress Framework	means the redress framework that will be established if the Digital ID Amendment Rules are passed.
sensitive information	has the meaning given in section 6 of the Privacy Act.
System Administrator	means the Chief Executive Centrelink, within the meaning of the *Human Services (Centrelink) Act 1997* (Cth).
transferring entity	if the Digital ID Amendment Rules are passed, means, in the context of streamlining applications, a relying party approved for participation in the AGDIS.
Trustmark	means the Digital ID Accreditation Trustmark.

Attachment 1 Materials Reviewed

This Attachment sets out a list of materials provided to Maddocks in connection with our conduct of this PIA. It does not include additional publicly available materials, including legislation, guidance and research materials, that we also considered as part of this PIA.

1. EXPOSURE DRAFT Digital ID Amendment (Redress Framework and Other Measures) Rules 2025 (provided to Maddocks on 4 September 2025).
2. EXPOSURE DRAFT Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025 (provided to Maddocks on 4 September 2025).
3. DRAFT Explanatory Statement – Digital ID Amendment (Redress Framework and Other Measures) Rules 2025 – Sep 2025 (provided to Maddocks on 9 September 2025).
4. DRAFT Explanatory Statement – Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025 – Sep 2025 (provided to Maddocks on 9 September 2025).
5. Digital ID Amendment (Redress Framework and Other Measures) Rules 2025 (version to be provided to the Minister) (provided to Maddocks on 3 November 2025).