Maddocks

Department of Finance

Privacy Impact Assessment

Digital ID Bill and Rules

Date of analysis – 20 October 2023

Date of finalisation – 18 December 2023

Part A Executive Summary

1. Introduction

1.1 On 19 September 2023, the Australian Government released an exposure draft of the Digital ID Bill 2023 (**Bill**). The Bill, if enacted, will establish a framework for an economy-wide voluntary accreditation for providers of various services in connection with the establishment and authentication of an individual's 'digital identity', which is an electronic representation that enables them to be sufficiently distinguished when interacting online with services (**Digital ID**).

1.2 At the same time, the Australian Government also released exposure drafts of two sets of rules which would be made under the Bill if it is enacted, being the Digital ID Rules 2024 (**Digital ID Rules**) and the Digital ID Accreditation Rules 2024 (**Accreditation Rules**) (together referred to as the **Rules**).

1.3 The proposed legislative framework will build upon and strengthen the existing voluntary (and non-legislated) scheme for accreditation of providers of Digital ID services, which is based on the existing Trusted Digital Identity Framework (**TDIF**). The Bill and Rules will provide for a phased expansion of the Australian Government Digital ID System (**AGDIS**), to include both government and non-government entities. Together, the legislative framework for the accreditation scheme for Digital ID providers and the phased expansion of AGDIS is referred to in this privacy impact assessment (**PIA**) as the **Digital ID System**.

1.4 The Bill will also establish the Australian Competition and Consumer Commission (**ACCC**) as the independent **Digital ID Regulator**. The Digital ID Regulator will be responsible for:

1.4.1 accrediting Digital ID entities in respect of their Digital ID services;

1.4.2 overseeing and maintaining the AGDIS, including approving which entities can participate in the AGDIS; and

1.4.3 using its legislative investigative and compliance powers to ensure Digital ID providers and services comply with the strict legislative requirements.

1.5 The Information Commissioner will regulate the privacy-related aspects of the accreditation scheme. This includes:

1.5.1 undertaking assessments in relation to the handling of personal information;

1.5.2 taking action in relation to certain breaches of the Digital ID System that will be taken to be an interference with the privacy of the individual under the *Privacy Act 1988* (Cth) (**Privacy Act**);

1.5.3 handling notifications by accredited entities under the Notifiable Data Breaches Scheme under the Privacy Act (which is extended to cover entities not otherwise covered by the Privacy Act or a comparable State or Territory scheme);

1.5.4 being involved in consultation about whether an entity should be accredited, and before the making or amendment of Rules that relate to privacy; and

1.5.5 providing advice to the Digital ID Regulator on request, on matters relating to the operation of the Digital ID System.

1.6 The Department of Finance (**Department**), as the Australian Government agency with key responsibility for the Bill, is committed to continuing its 'privacy by design' approach to developing the legislative framework for the Digital ID System. Accordingly, it has commissioned Maddocks to undertake this PIA, to consider whether the privacy impacts of the proposed legislative scheme have been identified and appropriately managed or minimised in the design of the accreditation framework and AGDIS.

2. This Privacy Impact Assessment Process

2.1 The Bill and Rules will involve the handling of personal information which is highly sensitive and where there are likely to be significant adverse privacy impacts for individuals if that personal information is mishandled or disclosed without authorisation. Undertaking this PIA is therefore 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 that are likely to have a significant impact on the privacy of individuals.

2.2 PIAs in respect of proposed new 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 the Australian Privacy Principles (**APPs**) in the 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 PIAs such as this one, which require consideration of a proposed new Australian law, the question then becomes whether the proposed Australian law *should* provide that authorisation.

2.3 Therefore, this PIA 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 and which are supported by Australian and international privacy best practice.

2.4 It is important to recognise that development of the Bill and Rules is a culmination of many years of policy consideration and detailed consultation with stakeholders and the broader public. A series of other independent PIAs have already been undertaken to inform the development of the Bill and Rules.[1] We have taken this previous work into account when undertaking this PIA.

2.5 In addition, the Department has run a public consultation process on the Bill and Rules in parallel with the PIA process, and we have also taken into account relevant feedback from this process which has been provided to us.

2.6 The Australian Government is currently reviewing the Privacy Act, and while at this stage it is not clear what changes may be implemented, this PIA has also taken into consideration these potential reforms. Further details about our methodology and assumptions is set out at **Attachment 1**. A glossary of defined terms and acronyms is at **Part D [Glossary].**

2.1 This PIA:

2.1.1 considers how the Bill, Digital ID Rules and the Accreditation Rules 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.

[1] '*Initial Privacy Impact Assessment for the Trusted Digital Identity Framework Alpha*' (2 December 2016) Galexia; '*Second Independent Privacy Impact Assessment for the Trusted Digital Identity Framework Alpha*' (September 2018) Galexia; '*Third Independent Privacy Impact Assessment on the TDIF and related Digital Identity Eco-Systems*' (September 2020) Galexia; and '*Digital Transformation Agency - Privacy Impact Assessment Report*' (8 February 2022) HWL Ebsworth Lawyers.

3. Summary of Findings

3.1 It will be critical that the privacy protections in the Bill and Rules are sufficient to engender public trust in the Digital ID System, because there will be serious negative impacts for people if their identity information (including sensitive biometric information) is misused or disclosed without authority. These impacts can include:

3.1.1 the heightened risk of identity theft – which could lead to financial fraud or loss, or the use of a person's identity by criminals;

3.1.2 potential risks to personal safety; and

3.1.3 psychological distress.

3.2 In our view, a commitment to a 'privacy by design' approach has been shown in the development of the Bill and Rules. The commitment to this approach can also be seen throughout the Bill and Rules, including the objects of the Bill in cl 3.

3.3 The Department and other Australian Government agencies with previous responsibility for the Digital ID System[2] have worked iteratively with stakeholders to develop the Bill and Rules. Stakeholder comments made in relation to the previous exposure drafts released in 2021 have also been taken into account. We have also found that many of the previous PIA findings and recommendations have been incorporated into the Bill and Rules.

3.4 The Bill and Rules include a range of strong privacy protection measures designed to minimise the potential privacy impacts of the new System, including:

3.4.1 extending the application of the Privacy Act to accredited entities who would not otherwise be covered, or ensuring that equivalent obligations are imposed;

3.4.2 including a person's attributes (which is broadly defined in the Bill to mean information that is associated with an individual, including information derived from another attribute) within the definition of 'personal information', even if that information would not otherwise be not covered by that definition in the Privacy Act;

3.4.3 a range of bespoke privacy safeguards, which provide control to individuals about how information (including biometric information) associated with them is collected, used, and disclosed;

3.4.4 data localisation for Digital IDs handled as part of the ADGIS – which means no personal information about persons can be transferred outside of Australia (except where an exemption has been granted by the Minister, which can only occur if particular requirements are met); and

3.4.5 a range of measures that entities must implement to gain and maintain accreditation (such as undertaking regular security assessments, conducting PIAs, and complying with reporting requirements).

3.5 The Bill also includes significant civil penalty provisions, designed to have a strong deterrent effect on entities, which can be enforced by the Digital ID Regulator or Information Commissioner.

3.6 As can be seen in the table in paragraph 14 in **Part C [Privacy Analysis]**, we consider that the legislative framework will address many of the privacy risks associated with the Digital ID System, and will provide individuals who choose to use a Digital ID with greater protections than are currently afforded under the TDIF.

[2] The Digital Transformation Agency had responsibility for the TDIF and the Digital ID Scheme until recently.

3.7 However, we have identified the following (though difficult to quantify) privacy risks, which we consider could benefit from further consideration:

3.7.1 **Risk 1**: Individuals and entities participating in the Digital ID System should expect consistency and certainty of key concepts across all Commonwealth legislation which regulates privacy and identity verification. There is a risk that the protections in the Bill may become out of step with the protections in the Privacy Act, particularly if the anticipated privacy reforms are enacted. In particular, we have concerns about the definition of 'personal information' in the Bill, and the potential impact of any reforms to this definition in the Privacy Act.

If this risk is not addressed, it may lead to potential confusion for participants in the Digital ID System, and the public at large, about what accredited entities are required to do, and may also impact on the effective regulation of the scheme.

3.7.2 **Risk 2**: Although the Bill and Rules contain detailed requirements and obligations, there is a risk that without further clarification about some concepts or obligations, different approaches will be taken by entities which may negatively impact on how personal information is handled.

This risk is particularly apparent in relation to protections in the Bill where the accredited entity must obtain the 'express consent' of the relevant individual. It is not clear that this includes a requirement to ensure all the best-practice elements for a valid consent are met (i.e., that it must be voluntary, informed, current and specific, unambiguous, and from someone with capacity to consent).

The following are other examples where further clarification could be provided: the intended meaning of 'collecting', 'disclosing' and 'holding' of personal information, particularly where there is recognition that cloud services are likely to be used; whether State and Territory privacy legislation is 'comparable' to the Privacy Act (or its data breach notification scheme comparable to that in Part IIIC of the Privacy Act); what is intended to be covered by 'intentional' collection of attributes in cl 41 of the Bill, and what steps an accredited entity should take before disclosing personal information to a relying party, in order to be satisfied they have met the 'data minimisation' requirements in the Accreditation Rules.

3.7.3 **Risk 3:** The proposed legislation incorporates a robust accreditation scheme, however some additional measures could potentially be included to further enhance the intended privacy protections. In particular, there is a risk that the Digital ID Regulator will not be able to take into account any findings or determinations of State and Territory privacy regulators in its accreditation-related decisions, and it is not clear how accredited entities are required to report to the Digital ID Regulator about their implementation of any PIA recommendations.

3.7.4 **Risk 4:** Given the nature of the personal information that will be handled as part of the Digital ID System, failure to quickly resolve a complaint could significantly increase the likelihood and/or consequences of the adverse impacts of any mishandling or unauthorised disclosure. It will be important that the co-regulators of the Digital ID System (the Digital ID Regulator and the Information Commissioner) are properly funded and work together in a seamless fashion, to ensure that individuals with a Digital ID can obtain efficient and effective handling of any privacy complaint.

3.8 The recommendations set out in paragraph 4.1 are designed to address the above risks, and further enhance the privacy protections in the proposed legislative framework and/or further strengthen privacy arrangements from a best practice perspective.

4. Recommendations

4.1 This PIA makes the following recommendations in relation to the Bill and Rules:

Recommendation 1 Clarifying meaning of 'personal information'

Rationale

The Bill provides a standalone definition of 'personal information' at cl 9 which in substance replicates the current definition of 'personal information' in the Privacy Act, and extends the definition to include 'attributes' (as defined) of individuals. However, given the language in cl 33 of the Bill (which extends the operation of the definition of personal information in the Privacy Act), there may be some uncertainty about whether the definition of 'personal information' is intended to be fixed as at the enactment of the Bill.

The Australian Government released its response to the Privacy Act Review Report in September 2023 which included an in principle agreement to adopt a more expansive concept of 'personal information' in the Privacy Act, to effectively include some technical and inferred data (e.g., IP addresses and other device identifiers).

There is a risk that the Privacy Act and the Bill may become misaligned in respect of information that will be 'personal information' under the Privacy Act in future, but not otherwise picked up in the meaning of 'attribute' in the Bill.

Recommendation

We **recommend** that the Department consider refining the drafting of the Bill to:

- define personal information in cl 9 of the Bill to simply reference the definition in the Privacy Act (which may change over time), so that cl 33 will then operate to include 'attributes' to the extent not already covered by any expanded definition; or
- make it clear whether the intention is to have a fixed definition of personal information as it is currently in the Privacy Act (but as extended to include attributes).

In either case, we suggest that the Explanatory Memorandum to the Bill clearly explain whether the intention is for the definition of personal information to change as the definition in the Privacy Act is updated following any Privacy Act reforms or not, and why that policy position has been taken.

Recommendation 2 Matters to be taken into account for accreditation – other privacy breaches

Rationale

Safeguarding the personal information of individuals is key to ensuring that there is social licence for the Digital ID System. In this context, if an entity breaches the privacy of an individual in respect of any of its other services and functions (whether under the Privacy Act or other legislation), this should be able to be taken into account by the Digital ID Regulator when considering whether or not to accredit that entity for the provision of Digital ID services, and also in decisions about whether or not that accreditation should be maintained.

The Digital ID Rules already provides for this to be taken into account in relation to entities that have been subject to certain Information Commissioner determinations under the Privacy Act or similar determinations under a similar law of a foreign jurisdiction (see Rule 5(1)(c) of the Digital ID Rules). However, this would not extend to any finding or determination of a State or Territory privacy regulator. We consider that ensuring that this can be taken into account as part of the accreditation process would provide further assurance to the Australian public that all entities participating in the Digital ID System are considered 'safe' to handle personal information in the context of the accredited service.

Recommendation

We **recommend** that the Department consider expanding Rule 5(1)(c) of the Digital ID Rules so that the Digital ID Regulator may also have regard to findings and determinations of a similar nature of a State or Territory privacy regulator.

Recommendation 3 Guidance on concepts included in the Bill

Rationale

In addition to the Information Commissioner's functions under the Privacy Act, clause 40 of the Bill sets out that an additional function of the Information Commissioner is to provide advice on request of the Digital ID Regulator on matters relating to the operation of the Bill. Section 28 of the Privacy Act provides for the Information Commissioner's guidance related functions under the Privacy Act. All the powers conferred on the Information Commissioner under the Privacy Act equally apply to the Digital ID System.

Stakeholders have raised a number of concerns during the consultation period about the meaning of certain concepts in the Bill, and we agree that ensuring that accredited entities can understand their obligations under the legislative framework will be key to ensure that the privacy protections are implemented in practice. This is particularly the case for some privacy protections in the Bill, such as ensuring that consent is obtained, which might be implemented by accredited entities anywhere along a compliance spectrum (from minimum requirements only, to full privacy best practice), particularly where the Bill does not define these terms, or import relevant concepts under the Privacy Act.

Recommendation 3 Guidance on concepts included in the Bill

We see benefit in the Information Commissioner issuing guidance on privacy matters related to the Digital ID System, particularly if language in the Bill and Rules is not further clarified. For example, guidance could be provided on the requirements for valid 'consent' in the various contexts of the Digital ID System, the proper interpretation of 'collect', 'disclose' and 'hold' in the Bill and Rules, the meaning of 'intentional' collection, and what steps an accredited entity should take before disclosing personal information to a relying party.

We believe such guidance would be particularly helpful by ensuring compliance with privacy best practice during the period before introduction of proposed reforms to the Privacy Act. We think this would benefit individuals using their digital ID under the Digital ID System, and minimise the adverse effects on the privacy of individuals.

Recommendation

We **recommend** that the Department work with the Information Commissioner to consider the stakeholder feedback provided during the consultation period, particularly on the meaning of different concepts in the Bill which stakeholders considered could benefit from being further defined or having guidance provided, to inform the Information Commissioner's approach to preparing any specific guidance in relation to the Digital ID System**.**

Recommendation 4 Arrangements between the co-regulators

Rationale

We expect the Digital ID Regulator and the Information Commissioner will work cooperatively in administering the Digital ID System. However, it will be important to ensure that individuals who are aggrieved have a seamless experience in having their complaints addressed.

Recommendation

We **recommend** that consideration be given to whether additional measures are required to facilitate the co-regulated nature of the Digital ID System. For example:

- providing in the Bill that the Digital ID Regulator and the Information Commissioner will develop a Charter setting out the commitments of the Digital ID Regulator and the Information Commissioner in undertaking their respective regulatory functions, including flows of information where one receives a complaint that is more appropriately handled by the other;
- the Department work with the Digital ID Regulator (once established) and the Information Commissioner to ensure there are appropriate administrative arrangements in place about how the co-regulators will work together and ensure there is publicly available information about this.

Recommendation 5 Accredited entities reporting on PIA implementation

Rationale

The Accreditation Rules require accredited entities to undertake PIAs in certain circumstances and provide their responses to any recommendations (and we see these as important privacy protections). However, there does not appear to be a mechanism to monitor whether an accredited entity has in fact undertaken any steps that it has indicated that it will do in response to a PIA recommendation. This may undermine the otherwise robust process.

Recommendation

We **recommend** that the Accreditation Rules provide that an accredited entity is required to report on the implementation of any actions it has indicated it will undertake in a response to a recommendation in a PIA (for example, as part of the annual review process).

Recommendation 6 Requirements for express consent

Rationale

In various different contexts, the Bill and Rules require that the 'express consent' of the individual is required to authorise the handling of personal information, however this wording is not currently included in some provisions, which may imply that implied consent is sufficient. We understand that this is not consistent with the policy intent.

Recommendation

We **recommend** that the drafting of the Bill and Rules be reviewed to ensure that all instances where consent of an individual is required refer to a requirement for 'express consent' (see for example clauses 46(3)(b), 47(2)(b) and 47(5)(c)(ii)).

Part B Project Description

5. Outline of this Part

5.1 In this Part, we summarise the key elements of the Digital ID System to be established through the proposed legislative framework. References to the proposed legislative provisions are as that set out in the exposure drafts released on 19 September 2023. Copies of these exposure drafts of the Bill, the Digital ID Rules and the Accreditation Rules can be found at Australia's Digital ID System website: https://www.digitalidentity.gov.au/have-your-say.

5.2 The Department has also prepared plain English language guides, *Factsheet: Digital ID legislation*; *Your guide to the Digital ID legislation and Digital ID Rules*; and *Your guide to the Digital ID Accreditation Rules*, which can also be found on the consultation section of the website.

5.3 The Digital ID System is described in detail in the above documents. In this Part, we have not sought to replicate all of that information, but rather to provide a high-level overview which explains concepts that are relevant to, and support the analysis in, **Part C [Privacy Analysis]** below. We have not sought to include or discuss every provision in the legislative framework, or all details about each of the provisions that are discussed below (for example, where a requirement is subject to exceptions, we have not listed every exception that might apply).

6. High Level Overview of the Digital ID Bill

6.1 A Digital ID of an individual means a 'distinct electronic representation of the individual that enables the individual to be sufficiently distinguished when interacting online with services' (Bill, cl 9). A Digital ID is intended to enable people to securely verify their identity online, so that they can receive a service without having to share copies of their sensitive identity documents.

The Digital ID System

6.2 Australians can currently use the Australian Government's accredited digital identity provider, myGovID, to access over 130 online Australian Government, and State and Territory government services. The current TDIF is an accreditation framework for digital identity services. It sets out rules around privacy, security, transparency, trust, and choice, which must be met for an entity to achieve accreditation and participate in the Australian Government's Digital ID System (currently only government agencies and government digital identity services can be onboarded to the System).

6.3 The Bill establishes a Digital ID Scheme involving:

6.3.1 a voluntary accreditation scheme of Digital ID service providers, building on the TDIF; and

6.3.2 a phased expansion of AGDIS, initially based around government services which will be expanded in phases to include participating private sector organisations.

6.4 Under the Bill, creating and using a Digital ID is voluntary (though the Digital ID Regulator will have the power to make exemptions to this in certain circumstances) (Bill, cl 71). Australians who cannot or do not want to use a Digital ID can continue to access government services over the phone or face-to-face at government shopfronts.

Accreditation Scheme

6.5 The AGDIS is a network of entities that provide or use Digital ID services in delivering participating government and commercial services. Participants will include:

6.5.1 **'accredited entities'**, who can provide Digital ID services; and

6.5.2 '**relying parties**', who can offer access to their services using a Digital ID (but they must generally also provide a non-Digital ID option for access to those services).[3]

6.6 The Bill proposes three types of accredited entities:[4]

6.6.1 **identity service providers**, who will help an individual set up or manage a Digital ID;

6.6.2 **attribute service providers**, who will verify and manage '**attributes**' (which as discussed below are pieces of information associated with the individual); and

6.6.3 **identity exchange providers**, who will facilitate interactions and information flow between identity service providers, attribute service providers, and relying parties in a Digital ID system.

6.7 Once accredited, the services provided by those entities under the Digital ID System are collectively referred to as the '**accredited services**'.[5]

6.8 The Bill provides a scheme for accrediting these entities.[6] It also provides for the creation of a new regulator, the **Digital ID Regulator** (which initially will be the ACCC), which will be responsible for accrediting and regulating accredited entities. The Bill also provides for the role of a **Digital ID Data Standards Chair**, which will be responsible for setting and publishing nationally consistent data standards used in the Digital ID System (such as about technical integration requirements, design features, and potentially also test standards). These will include service levels for the provision of Digital ID services, and Data Standards will be able to be made in future, for example to cover emerging technologies such as verifiable credentials and digital wallets.

Compliance requirements for accredited entities

6.9 An accredited entity must comply with **privacy safeguards** (which are discussed further below), as well as conform with additional consumer protections in the Bill, including:

6.9.1 de-activation of a Digital ID upon request (Accreditation Rules, r 5.7);

6.9.2 ensuring services are accessible and inclusive (Bill, cl 29);

6.9.3 not holding, storing, handling or transferring system information outside Australia (unless an exemption applies) (Bill, cl 73);

6.9.4 generally, keeping records for seven years, or three years if accreditation has been revoked (Bill, cl 129(4)(b));

6.9.5 producing an annual report that includes changes made to the entity's Digital ID data environment, results of assurance assessments and systems testing, and attestation that the entity has reviewed its system security and fraud control plan (Bill, cl 27(2)); and

6.9.6 complying with key reporting obligations to the Digital ID Regulator (Bill, cl 27(2)).

[3] See the definition of 'relying party' is defined in cl 9, and the general rule and exceptions in cl 71 of the Bill.
[4] Again, definitions for these types of entities are set out in the Bill, and the descriptions in this paragraph are intended to be a summary of those definitions only.
[5] See the definition in cl 9 of the Bill.
[6] See Bill, Chapter 2.

Key definitions

6.10 The Bill extends the definition of '**personal information**' to ensure it includes attributes of individuals that are not otherwise included in the definition under the Privacy Act (Bill, cl 9, definition of 'personal information').

6.11 An '**attribute**' is information associated with an individual, and expressly includes (among other things) the individual's name, date of birth, address, passport or licence numbers, and the time and date a Digital ID was created. It also includes information that can be derived from another attribute. Generally, attributes such as these would be considered personal information if connected to an identified individual. However, the Bill will extend the meaning of personal information to attributes, even if they do not relate directly to an identifiable individual.

6.12 The Bill restricts or prohibits the collection, use or disclosure of certain attributes. Those attributes are described as:

6.12.1 **Restricted attributes**: These attributes are subject to additional protections in the Bill, and include 'health information' as defined in the Privacy Act, government identifiers (such as a tax file number or Medicare number), information or an opinion about a person's criminal record, membership of a trade union or professional or trade association. Additional restricted attributes may be prescribed in the Digital ID Rules after consultation (Bill, cl 11).

6.12.2 **Prohibited attributes**: These are attributes that accredited entities are not permitted to intentionally collect, use or disclose, and include information or an opinion and an individual's racial or ethnic origins, political opinions or membership of a political party, religious beliefs or affiliations, philosophical beliefs or sexual orientation or practices.[7] The restriction does not extend to 'unintentional' handing of this information, given that collection of a photograph might unintentionally also disclose their religious beliefs because of their clothing (Bill, cl 41).

Privacy safeguards

6.13 The Bill contains additional privacy safeguards which are specific to the management of Digital IDs by accredited entities(see Bill, Chapter 3, Part 2.). Accredited entities:

6.13.1 as discussed above, must not intentionally collect, use or disclose prohibited attributes (cl 41);

6.13.2 must not disclose certain attributes of an individual to a relying party without the express consent of that individual (these include that person's name, address, date of birth, phone number or email address) (cl 42);

6.13.3 unless it is a condition of their accreditation, must not disclose restricted attributes to a relying party without express consent of that individual (cl 43);

6.13.4 are subject to restrictions on disclosing an individual's unique identifier that has been assigned to an individual, except in the particular circumstances in the Bill (e.g., if necessary for the detection of fraud or where disclosure facilitates access to a service using their Digital ID) (cl 44);

6.13.5 must abide by strict limits on the collection, use, disclosure and retention of biometric information, which generally limit the use of biometric data by accredited entities to particular identity verification and authentication purposes, and impose strict time limits for destruction of biometric information (cl 46, 47 and 48). The Bill also makes provision for the Accreditation Rules to govern emerging issues involving biometric information (cl 49);

6.13.6 are expressly prohibited from using biometric information to undertake 'one-to-many matching' (that is, comparing a biometric profile of one individual against that of many others to identify that individual) – the Digital ID System is intended to only permit 'one-to-one matching' (that is, comparing a biometric profile of one individual against one other stored profile for that individual, to determine whether there is a match) (cl 45);

[7] See Bill, cl 41.

6.13.7 are prohibited from data profiling to track online behaviour, unless an exception applies (exceptions include the provision of the accredited services, such as improving the performance or useability of the entity's IT system), or demonstrating compliance with their obligations under the legislative framework) (cl 50);

6.13.8 are subject to restrictions on the disclosure of personal information to a law enforcement body (the restrictions mean that the circumstances for disclosure are narrower than the equivalent provisions under the Privacy Act, which permits disclosure of personal information to an enforcement body if reasonably necessary for an 'enforcement related activity'[8]) (cl 51);

6.13.9 must not use or disclose personal information for marketing purposes unrelated to the Digital ID service provided, regardless of whether or not the individual consents (cl 52); and

6.13.10 must not retain particular attributes of an individual (including their name, address, date of birth, phone number, email or restricted attributes) after the authentication session is complete (cl 53).

6.14 In addition, the Bill provides for:

6.14.1 further data breach notification obligations to the Digital ID Regulator, which are in addition to existing notification requirements to the Information Commissioner in the event of an eligible data breach under the Privacy Act, requiring notification to the Digital ID Regulator of any 'cybersecurity incident' that includes:

(a) unauthorised access or attempted access to a system, service or network; and

(b) unauthorised impairment of, or an attempt to impair, the availability, reliability, security or operation of a system, service or network;

6.14.2 additional obligations to separately provide any notice of an eligible data breach to both the Digital ID Regulator and the Information Commissioner; and

6.14.3 a requirement to notify individuals of a cyber incident or risk in the Digital ID system that is likely to adversely affect individuals using the accredited services.[9]

Regulatory powers

6.15 Under the Bill, the Digital ID Regulator may revoke or suspend an entity's accreditation, including if:

6.15.1 the entity contravenes its obligations under the legislative framework[10];

6.15.2 the entity has, or will be, involved in a cyber security incident;

6.15.3 the national security interest supports the decision; or

6.15.4 the Digital ID Regulator is satisfied that the entity is no longer appropriate (with consideration of whether the entity is a fit and proper person).[11]

6.16 The Information Commissioner will have regulatory oversight over the privacy-related aspects of the Digital ID System. Both the Digital ID Regulator and the Information Commissioner may seek civil penalties, with a specific penalty regime split between the co-regulators. The Bill provides the Digital ID Regulator with relatively typical powers to monitor and enforce compliance, including to give directions, compel production of a document or information, and issue a compliance notice. The Information Commissioner may also issue an infringement notice, seek enforceable undertakings and seek injunctions on matters relating to the privacy safeguards. Decisions of the Digital ID Regulator may be subject to review, including by the Administrative Appeals Tribunal.

[8] See *Privacy Act 1988* (Cth), APP 3.4(d)
[9] See Accreditation Rules, r 4.27 and 4.28.
[10] Clause 26 of the Bill refers to a breach of 'this Act', which is broadly defined in cl 9 and includes the Bill, Digital ID Rules, Accreditation Rules, the Digital ID Standards and service levels determined by the Digital ID Standards Chair.
[11] See Bill, cl 26.

7. High Level Overview of Digital ID Rules

7.1 The Digital ID Rules will be made by the Minister and will be disallowable by Parliament. They provide additional requirements for entities participating in the AGDIS.

7.2 They will include:

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

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

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

7.2.4 when the interoperability obligations in the Bill (at cl 75) will apply;

7.2.5 the information to be included by entities when reporting:

(a) a cyber security incident (as defined in the Bill);

(b) a Digital ID fraud incident (as defined in the Bill),

which they are required to do under cl 74(1) of the Bill;

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

7.2.7 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 its Digital ID services).

8. High Level Overview of Accreditation Rules

8.1 The Accreditation Rules will be made by the Minister and will be disallowable by Parliament. They will set out the requirements for entities obtaining and maintaining accreditation under the Bill.

8.2 Key requirements for obtaining and maintaining accreditation include the following:

8.2.1 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);

8.2.2 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);

8.2.3 undertaking assurance assessments and systems testing, both on application and on an annual basis[12], including:

(a) a protective security assessment against standards such as ISO 27001, 27002 or 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;

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

(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

8.2.4 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.

Part C Privacy Analysis

9. Outline of Part

9.1 Legislative schemes can override requirements contained in the Privacy Act, because the Privacy Act expressly allows some acts and practices that would otherwise be prohibited under the Privacy Act to be undertaken if they are 'authorised or required' by law (see APP 3.4(a) in relation to the collection of sensitive information, and APP 6.2(b) in relation to the use or disclosure of personal information for a secondary purpose). Similarly, legislative schemes can impose privacy safeguards that will apply in addition to those contained in the Privacy Act.

9.2 This means that there is little utility in considering a new legislative scheme such as the Bill and Rules from a compliance perspective against the existing requirements in Privacy Act. Instead, in this Part we use the APPs as a framework to consider, from a principles basis, the privacy impacts of the Digital ID System proposed in the Bill and Rules, to continue the 'privacy-by-design' approach that has been taken to date in connection with the development of this legislation.

9.3 The development of the Bill and Rules is a culmination of many years of policy consideration and stakeholder and broader public consultation[13], informed by a series of PIAs[14]. In this Part, we do not seek to repeat issues that have been raised in the previous PIAs and already considered as part of the development of the Bill. Nor do we consider the broader policy issues, such as whether a Digital ID System should be introduced at all, which a number of stakeholders raised concerns about during the consultation period for the Bill.

9.4 Rather, this Part considers the proposed Bill and Rules and sets out:

9.4.1 some threshold privacy issues for the Digital ID System, including:

(a) interaction with the Privacy Act;

(b) collection, use and disclosure of biometric information; and

(c) regulatory oversight of the Digital ID System; and

9.4.2 a table which considers the privacy impacts of the Bill and Rules against each APP, to:

(a) illustrate the steps that have already been taken to address each APP in the Bill and Rules; and

(b) set out a 'gap analysis' which identifies where we consider that there are additional strategies which could be considered to further minimise or mitigate the identified privacy impacts.

[13] The Australian Government released a precursor to the current legislative package for Digital ID in 2021, which included exposure drafts for the Trusted Digital Identity Bill 2021, Trusted Digital Identity Framework Accreditation Rules and Trusted Digital Identity Rules. The previous exposure drafts and submissions can be found at: https://www.digitalidentity.gov.au/previousconsultations

[14] *Initial Privacy Impact Assessment for the Trusted Digital Identity Framework Alpha*' (2 December 2016) Galexia;
'*Second Independent Privacy Impact Assessment for the Trusted Digital Identity Framework Alpha*' (September 2018) Galexia; '*Third Independent Privacy Impact Assessment on the TDIF and related Digital Identity Eco-Systems*' (September 2020) Galexia; and '*Digital Transformation Agency - Privacy Impact Assessment Report*' (8 February 2022) HWL Ebsworth Lawyers.

10. Interaction with the Privacy Act

10.1 We consider that the measures in the Bill and Rules to ensure that accredited entities comply with the protections in the Privacy Act are commendable. We also strongly support providing additional targeted privacy requirements in the Bill which are tailored to the specific issues that arise in the context of the Digital ID System.

10.2 Stakeholders have also commented on the need for holistic consideration of all Commonwealth legislation about handling of information about a person's identity (including the Digital ID System, reforms to the Privacy Act and the Identity Verification Services Bill 2023), to ensure there is consistency in how personal information (particularly biometric information) is regulated. While a full examination of this issue is beyond the scope of this PIA (which is focussed only on the Digital ID System), we have particularly considered the interaction between the Privacy Act, and the Bill and Rules.

Meaning of 'personal information'

10.3 The Bill expands the current definition of 'personal information' contained in the Privacy Act for the purposes of the Digital ID System to include 'attributes' of individuals (see paragraphs 6.10 - 6.12 above). In our view, this expansion to include attributes, which are not necessarily linked to an identifiable individual, affords greater protection to information associated with an individual. It means that the privacy protections in the Bill and Rules will apply to a wider range of information, which might not be protected under the Privacy Act.

10.4 A number of stakeholders have raised the need for consistency across all Commonwealth legislation dealing with personal information. In particular, at this stage it is not clear to what extent proposed reforms to the Privacy Act may impact the Digital ID System.

10.5 The Australian Government has indicated its intention to introduce legislation in 2024 to implement Privacy Act reforms. In its *Government Response to the Privacy Act Reform Report*[15], the Australian Government has:

10.5.1 'agreed in-principle' to clarify the scope of personal information in the Privacy Act, including to add a non-exhaustive list (see *Proposal 4.1*). This change is likely to bring a range of additional technical information and inferred information within the scope of the definition (but it is not yet clear whether or not all of this additional information would also meet the definition of 'attributes' in the Bill, and therefore be incorporated into the definition of 'personal information' in the Bill); and

10.5.2 clarified its view that an individual's identity does not need to be known if an individual is able to be distinguished from all others. It flagged that this would be clarified through updates to the definition of 'personal information' in the Privacy Act and/or additional guidance by the Office of the Australian Information Commissioner (**OAIC**).

10.6 The Bill sets out at cl 9 a definition of 'personal information', which:

10.6.1 in paragraph (a) replicates in substance the current definition of 'personal information' in the Privacy Act - but does not refer to the Privacy Act itself (that is, it does not adopt the relatively common practice in other legislation of simply referring to the definition as set out in the Privacy Act); and

10.6.2 in paragraph (b), expressly includes attributes, to the extent that they are not already covered in paragraph (a).

10.7 Clause 33 of the Bill also extends the operation of the Privacy Act to cover attributes of individuals which are in the possession or control of accredited entities (by extending the definition of 'personal information' in the Privacy Act to include such attributes). That is, the Privacy Act will apply to accredited services provided by accredited entities where they handle attributes under the Bill, even if it those attributes would not otherwise be personal information within the meaning of the Privacy Act.

[15] Available from www.ag.gov.au.

10.8 However, it is not clear whether the following phrase in the Bill at cl 33, '*to the extent not already covered by the definition of personal information within the Privacy Act 1988, attributes of individuals…to be personal information about an individual*', read with the definition at cl 9, it is intended that the definition of 'personal information' is to be fixed as at the time the Bill is enacted. We therefore see a risk that the Privacy Act and the Bill may become misaligned in respect of information that will be 'personal information' under the Privacy Act in the future, but not otherwise picked up in the meaning of 'attribute' in the Bill.

10.9 This falls within **Risk 1** (see paragraph 3.7 in **Part A [Executive Summary]**).

10.10 In **Recommendation 1** we have set out options for the Department to consider, which are designed to address this potential risk.

Privacy obligations for non-APP entities

10.11 While the application of the Privacy Act is extended under the Bill to cover attributes of individuals, the Privacy Act only applies to 'APP entities'. This term does not currently cover the majority of small businesses (as defined) nor the majority of State and Territory entities. Some of these entities may wish to become accredited entities, but would not be otherwise subject to the requirements under the Privacy Act in respect of their handling of personal information in connection with the Digital ID System.

10.12 We consider that the Bill includes a significant privacy enhancing measure in including specific provisions which will apply to non-APP entities. Clause 34 will effectively mean that, even if an accredited entity is not an 'APP entity', they will not be permitted to handle personal information unless:

10.12.1 they are subject to Privacy Act as if they were an organisation under that Act (e.g., because of the operation of section 6E, 6EA or 6F of the Privacy Act);

10.12.2 they are subject to State or Territory law which has protection for personal information which is 'comparable' to the APPs[16]; or

10.12.3 the entity has an agreement (an **APP-equivalent agreement)** with the Commonwealth, which prohibits the entity from collecting, holding, using or disclosing personal information in a way that would breach an APP if they were an organisation under that Act.[17] We note that it will be important for the Commonwealth to ensure that the terms of this agreement are carefully drafted and otherwise appropriate (for example, if the agreement permitted the entity to terminate the agreement at any time, this may affect the ability of the Information Commissioner to later enforce its terms in accordance with the Bill).

10.13 In relation to the second of the options above, the Bill mirrors the approach taken under the *Data Availability and Transparency Act* (Cth). However, a common criticism and complaint amongst privacy practitioners and advocates is the lack of consistency in privacy laws across the different Australian jurisdictions. Although many privacy obligations in State or Territory privacy legislation are similar to those in the APPs (which is to be expected, given that they are based on the same general privacy principles), there are distinct and often important differences in the language used, and in how that language has been interpretated by the State and Territory regulators and the courts. It will therefore be important to understand when a State or Territory law is considered 'comparable'.

10.14 We appreciate that it may be impracticable for details of which laws are comparable to be included in the Bill and Rules, given the potential for State and Territory privacy laws to be introduced, changed, or repealed over time. Accordingly, we consider that there may be benefit in the Information Commissioner, as the regulator of both the Privacy Act and the privacy-related aspects of the Digital ID System, to provide guidance on which State or Territory privacy laws are considered to provide protections which are 'comparable' to the APPs. We consider this raises **Risk 2**, but that this could be addressed as part of implementing **Recommendation 3**.

[16] The State or Territory law must also provide for the monitoring of compliance with the law and a means for an individual to seek recourse under the law (see cl 34(2)(b) of the Bill).
[17] See definition in Bill, cl 32. These agreements are enforceable by the Information Commissioner as an interference with the privacy of the individual under the Privacy Act (see Bill cl 35).

Further matters to be considered by the Digital ID Regulator when accrediting entities

10.15 Confidence in the handling of personal information by accredited entities is at the heart of the Digital ID System, and necessary to garner trust and social licence. This means that measures should be put in place to ensure that only entities who have appropriate systems and procedures in place to handle personal information, and who have demonstrated that they can be trusted to do so properly and safely, should be accredited.

10.16 The Bill, Digital ID Rules and Accreditation Rules already have a number of important measures in place, including:

10.16.1 that the Digital ID Regulator must not accredit an entity in a range of circumstances, including if the entity does not meet the criteria for accreditation in the Accreditation Rules[18];

10.16.2 that the Digital ID Regulator may take into account a range of relevant factors when deciding whether or not to accredit and entity or approve their participation in the AGDIS, which are likely to impact on the ability and likelihood of the entity complying with the privacy and security requirements in the legislative framework. These expressly include that the Digital ID Regulator may take into account whether the entity is a 'fit and proper person'[19].

10.17 In determining whether the entity is a 'fit and proper person', the Digital ID Regulator must take into account certain matters[20]. One of these is whether an entity has previously been found to breach relevant privacy laws (including breaches in any of its undertakings, and not just in providing its accredited services), specifically whether they have been subject to certain determinations by the Information Commissioner under the Privacy Act, or similar findings or determinations under a similar law of a foreign jurisdiction.[21]

10.18 However, we were unable to see that the Digital ID Regulator is able to take into account any similar finding or determination made by a State or Territory privacy regulator[22]. This raises **Risk 3**, and may be relevant given the types of entities who may (particularly in the future) seek to become accredited. **Recommendation 2** is intended to further assist in assuring the Australian public that only entities who have a sound 'track record' are considered 'safe' to handle personal information in the context of the accredited service and permitted to participate in the Digital ID System.

11. Collection, Use and Disclosure of Biometric Information

11.1 The collection, use and disclosure of biometric information is one of the key concerns raised by stakeholders during the consultation period for the Bill. The OAIC's *Australian Community Attitudes to Privacy Survey 2023* (**ACAPS 2023**) found that:

> *Australians' level of comfort with biometric information being collected and used depends largely on the type of organisation and the context.*
>
> *Australians are most comfortable with the collection and use of their biometric information in border security and law enforcement contexts, and they are more likely to trust the public sector to collect and use this kind of information than businesses.*[23]

11.2 We note that, unlike the Privacy Act, the Bill provides a definition of 'biometric information' at cl 9, which we consider to be a positive privacy measure, as it provides a much clearer baseline for understanding of this term.

11.3 We consider including provisions in the Bill which specifically regulate the handling of biometric information to be appropriate, and takes into account general community concerns about the collection and use of biometric information and the more significant adverse impacts for individuals if this type of information is misused or disclosed without their authority.

[18] Bill, cl 15(4).
[19] Bill, cl 15(5), also cl 59
[20] Bill, cl 12 and Digital ID Rules, r 5.
[21] Digital ID Rules, r 5(1)(c).
[22] Defined in the Bill as a 'State or Territory privacy authority' (see cl 9 of the Bill).
[23] ACAPS 2023, p 10.

11.4 The Bill includes a range of safeguards on the use of biometric information by accredited entities, including:

11.4.1 biometric information can be collected and used for verification or authentication purposes, and can only be retained for those purposes and must be deleted after that use ceases (Bill, cl 45 and cl 46);

11.4.2 prohibiting one-to-many matching using biometric information – that is, a person's biometric information cannot be used by an accredited entity to compare against biometric information to identify the individual (Bill, cl 45(2)).

11.4.3 in relation to authentication, biometric information can be retained where the individual has consented to this so the biometric information can be used to authenticate the individual in the future;

11.4.4 only limited secondary uses of biometric information is permitted including:

(a) for fraud investigation and certain testing[24]. However, a biometric retained for fraud and testing activities must be deleted within 14 days of collection;

(b) disclosure to the individual;

(c) disclosure to law enforcement with a warrant issued by a magistrate, judge or tribunal; and

(d) disclosure to law enforcement with consent of the individual concerned for an investigation/prosecution or identity verification.

11.5 Many stakeholders are concerned about accredited entitles collecting biometric information and retaining any such information. In particular, stakeholders are concerned about the security risks with entities holding biometric information, as it represents a 'honey pot' for attacks by those with malicious intentions ('hackers'). We sympathise with these sentiments.

11.6 However, we consider the measures in the Bill (which sets out the limited circumstances in which biometric information can be retained, and then up to 14 days from collection) combined with the security measures (including regular security assessments) that accredited entities are required to undertake as part of obtaining and maintaining their accreditation, are reasonable measures to mitigate against the risk of data breach involving biometric information arising, including minimising any harm that may arise from a breach.

11.7 Many stakeholders were particularly concerned about accredited entities being able to disclose biometric information to law enforcement bodies. However, we appreciate that the right to privacy is not an absolute right and in certain circumstances it may be appropriate for the right to privacy to be subjugated. We note that the Privacy Act recognises this balancing act where it provides that one of the objects of the Privacy Act is to 'recognise the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities'.

11.8 We consider the requirements of requiring a warrant or the consent of the individual is a high bar that protects the privacy of the individual while recognising the legitimate reasons that law enforcement may require the biometric information in undertaking their functions.

12. Issues about consent

12.1 We believe that it is commendable that the Bill and Rules require that consent must be obtained from the relevant individual, in various different contexts. We support this as a measure that gives control to the individual about how their personal information will be handled. We particularly support the drafting which clarifies that such consents are required to be 'express consent'. In our view, this is a privacy enhancing measure because allowing reliance upon implied consent can be fraught with the potential for misunderstanding about the individual's actual intentions.

[24] See Accreditation Rules.

12.2 We note that clauses 46(3)(b), 47(2)(b) and 47(5)(c)(ii) of the Bills do not currently state that express consent is required. We recommend that, consistent with our understanding of the policy intent, that the drafting of the Bill and Rules be reviewed and updated as required (**Recommendation 6**).

12.3 Privacy advocates have long claimed that consent can be meaningless if individuals seeking a service are asked for consent, where the alternative, if consent is refused, is that the individual cannot access that service. The Bill has addressed this concern by ensuring that relying parties (at least those participating in the AGDIS) must not require an individual to create or use a Digital ID as a condition for providing their service or access to their service (Bill cl 71)[25].

12.4 However, we again note that the concept of 'consent' itself is not defined in either the Bill nor the Rules, and different entities are likely to have different ideas about the minimum standards that are required before consent is considered to be valid, and whether the consent is permitted to be 'bundled' with other consents. This raises **Risk 2**, which is likely to be more acute before the implementation of any proposed reforms to the Privacy Act (which include proposals to ensure that consent is voluntary, informed, current, specific and unambiguous, see *Proposal 11.1*).

12.5 Although the OAIC has provided guidance about the meaning of consent in the context of the APPs, we consider that there would be benefit in the OAIC providing guidance on the meaning of consent generally in the Digital ID System, as set out in **Recommendation 3**, and particularly in the context of the safeguards for the disclosure of biometric information.

12.6 In analysing the requirements to obtain consent, it is important to note that an accredited identity service provider must not generate, manage, maintain or verify information of an individual if they have not yet obtained the age of 15 years. This is consistent with guidance provided by OAIC[26], and is designed to ensure that individuals under the age of 18 years can be presumed to have sufficient capacity to understand what they are consenting to.

12.7 We understand that the Department is considering whether this age should be reduced to 14 years in line with the *Age Discrimination Act 2004* (Cth), particularly when young people aged 14 years may wish to interact with relying parties online using a Digital ID in connection with their employment or education. We think this is likely to be able to be justified from a privacy perspective, given:

12.7.1 that 14-year-olds who wish to engage in an online manner using their Digital ID are likely to be 'digital natives', and more likely to have a high degree of familiarity with using online platforms, and therefore be capable of understanding how their personal information will be used; and

12.7.2 the Accreditation Rules require identity service providers to provide individuals with a clear and simple description of each step of the identity proofing process (Accreditation Rules, r 5.33) – this will increase the likelihood that 14-year-olds will be provided with information to assist them to understand the journey map.

13. Regulatory Oversight of the Digital ID System.

13.1 The Digital ID System will be co-regulated with the Digital ID Regulator (the ACCC) and the Information Commissioner. The Bill outlines that the Digital ID Regulator can seek guidance from the Information Commissioner. The Information Commissioner is also to be consulted in respect of any changes to the Rules.[27]

13.2 We consider it appropriate for the Information Commissioner to have an oversight role in relation to the privacy aspects of the Digital ID System, as this will ensure a level of conformity in approaching privacy related issues across different schemes. It will be important for the OAIC and the ACCC to be funded and be provided with the necessary resources so that they may issue appropriate guidance material and undertake other educational activities, and to implement effective monitoring and enforcement regimes, to ensure that the protections in the legislative framework are effective.

[25] There are exceptions to this general rule, including where the entity is facilitating access by the individual to another entity's service, that that other entity offers access without creating and using a Digital ID through the AGDIS (cl 71(2)), or an exemption is provided by the Digital ID Regulator.
[26] APP Guidelines, Chapter B, paragraph B.59-61.
[27] Bill, cl 159(1)(b).

13.3 In a co-regulated environment, it will also be important to ensure that individuals who wish to make a privacy complaint, or otherwise seek assistance or redress in relation to the Digital ID System have access to a consistent and effective complaints management process. Under the Bill, the Digital ID Rules can provide for a redress framework (but they do not currently do so).

13.4 The Digital ID Regulator is given specific authorisations to use and disclose personal information in connection with its regulation of the Digital ID System (see Bill, cl 88-90), which we consider to be appropriate

13.5 Given that any alleged breach of the protections in the legislative framework is likely to need a time-critical response (for the individual alleging the breach, and any other individuals whose personal information is being handled by the accredited entity), it will be important that the two regulators are able to work together in an efficient way. Our **Recommendation 4** is intended to address **Risk 4** and provide some strategies to address this issue.

14. Table of Privacy Risks and Impacts, with Considerations Against the APPs

This table sets out the privacy principles behind each of the APPs, and identifies the potential privacy risks and impacts that may eventuate if those principles are not appropriately implemented in connection with the Digital ID System. The table then sets out the measures that have already been incorporated into the Bill and Rules to address those risks, and a gap analysis of whether any further steps could be taken. This table should be read in conjunction with the more detailed analysis in paragraph 13 above.

<table>
<tr><td colspan="2">Principles behind APP 1 - Open and transparent management of personal information

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.</td></tr>
<tr><td colspan="2">Potential privacy risks and impacts if these principles are not implemented for the Digital ID System

• Lack of transparency about how an entity handles personal information in relation to the Digital ID System has the potential to erode the Australian public's trust and confidence in the System (sometimes described as a 'social licence'). Given that the Digital ID System is voluntary, any lack of trust or confidence is likely to affect 'take up' by individuals, meaning that more people will continue to need to provide their identity documents to various entities (with the associated data breach risks and impacts for individuals which the Bill and Rules seek to avoid).

• Poor privacy governance practices, procedures and systems are likely to lead to poor management of personal information in connection with the Digital ID System, with the associated increase in adverse impacts for individuals when their personal information is mishandled.</td></tr>
<tr><th>Current measures in the Bill and Rules</th><th>Potential further steps</th></tr>
<tr><td>The Bill and Rules already include a number of important measures that promote the open and transparent management of personal information by accredited entities. These include requiring accredited entities to:

• Comply with the Privacy (Australian Government Agencies — Governance) APP Code 2017 (the Privacy Governance Code) or an instrument that replaces that code (Accreditation Rules, r 4.35). This Code already applies to agencies covered by the Privacy Act[28], and requires a dedicated Privacy Officer, Privacy Champion, privacy management plan, and register of privacy impact assessments. This measure will provide a common benchmark for best practice in privacy governance, so all accredited entities are managing personal information to a consistent high standard;</td><td>We consider the requirements set out in the Accreditation Rules (described in the previous column) are important protections and will assist in ensuring that accredited entities are handling personal information (including attributes of individuals and biometric information) in an open and transparent way.

We note that while under cl 6.7 of the Accreditation Rules, an accredited entity must provide the Digital ID Regulator annually with a report that contains particular information and documents, including a copy of any PIA involving the accredited entity's Digital ID data environment or accredited services and a copy of the entity's responses to the assessment (Accreditation Rules, cl 6.7(f)), it is not clear whether an entity must report on its implementation of those responses. In other words, although there are detailed requirements for the conduct of an</td></tr>
</table>

[28] The Rule is expressed to apply to accredited entities that are not an agency within the meaning of the Privacy Act.

• maintain a privacy policy specifically for the accredited services, in addition to any more general privacy policy for its other activities (Accreditation Rules, r 4.36); • annually review their privacy policy and privacy management plan (Accreditation Rules, r 4.37); • provide privacy awareness training to their personnel (Accreditation Rules, r 4.40); • create and make publicly available a journey map of information flows which is consistent with the entity's latest PIA (Accreditation Rules, r 4.49); and • conduct an independent PIA in accordance with the requirements at r 2.3 of the Accreditation Rules. We also see that the expansion of the notifiable data breach scheme in Part IIIC of the Privacy Act to accredited entities who would not otherwise be bound by that scheme, or by a comparable State or Territory scheme (see Bill, cl 37-39), is a further measure to ensure individuals are made aware of how their personal information has been handled (or mishandled) in relation to the Digital ID System. We also consider that is it appropriate for: • the Digital ID Regulator to publish registers of entities who are, or have been, accredited or approved to participate in the AGDIS, to be a further measure for individuals to understand any conditions or limitations imposed upon that entity in relation to its handling of their personal information (Bill, cl 116-117); and • the Digital ID Regulator and Information Commissioner to produce reports, for presentation to Parliament, about their operations during each financial year (Bill, cl 144 and 145) We see these as further mechanisms that will enhance openness and transparency for individuals.	independent PIA, and the entity must demonstrate an *intention* to implement any recommendations, we could not see a mechanism by which the regulator can be satisfied that those recommendations have in fact, been implemented. We **recommend** that consideration be given to including such a requirement in the Accreditation Rules to address **Risk 3** (see **Recommendation 5**).

Principles behind APP 2 - Anonymity and pseudonymity APP 2 is intended to allow individuals to interact with an entity without identifying themselves, or to use a pseudonym, unless to do so is not reasonable or is impracticable in the circumstances (or another law requires or authorises their identification).	
Potential privacy risks and impacts if these principles are not implemented for the Digital ID System We do not consider that there are any specific risks and impacts associated with APP 2 in respect of the Digital ID System, which is about ensuring individuals *can* identify themselves safely.	
Current measures in the Bill and Rules	**Potential further steps**
Providers of Digital ID services will need to know the identity of persons (it would be impracticable to provide Digital ID services without knowing the identity of the relevant individual),where the individual is a 'shielded person', for example because they are in a witness protection program – their identity will have been assumed and may not be 'real', but the Digital ID Regulator will need to be satisfied that the entity has appropriate procedures in place for dealing with those assumed identities (Bill, cl 59(2)). In a broad sense, the Bill promotes the principle behind APP 2 by making it clear that creating and maintaining a Digital ID is voluntary, so that individuals do not need to disclose their identity through the Digital ID System if they do not wish to (Bill, cl 71).	No further steps are proposed in respect of APP 2.

Principles behind APP 3 - Collection of solicited personal information

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).

Potential privacy risks and impacts if these principles are not implemented for the Digital ID System

- 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 the amount of personal information (including sensitive information and information that establishes a person's identity) that may be accessed by a malicious actor.
- For biometric information (which accredited entities must obtain the individual's consent to collect, unless it is otherwise authorised), there is a risk that individuals may not understand what they are being asked to consent to (i.e., entities may not be able to demonstrate that they have the valid express consent of individuals).

Current measures in the Bill and Rules	Potential further steps
The Bill prohibits the intentional collection of certain attributes of individuals (cl 41), including information which most people would consider particularly sensitive (such as an opinion about an individual's racial or ethnic origin, religious beliefs or sexual orientation or preferences). These listed attributes are a subset of 'sensitive information' under the Privacy Act. This restriction will aid in minimising the collection of this information, which has the likelihood of causing greater harm to individuals if mishandled or disclosed without authorisation. In addition, the Accreditation Rules expressly requires accredited entities to minimise the collection of personal information to that which is reasonably necessary to provide its accredited services (Accreditation Rules, r 4.38). The Bill also provides that biometric information can be collected for verification or authentication purposes by accredited entities, but only where the entity's conditions on accreditation specifically authorise the collection (Bill, cl 46(1)(b)). Further, express consent for the collection is required as the collection is not otherwise authorised by the provisions referred to in cl 45(1)(b). This restriction will limit the entities within the Digital ID System that can collect biometric information and the importance of obtaining consent. (Please see the discussion in APP 11 in	While we consider the measures in the Bill go some way to minimise the privacy risks and impacts associated with the collection of personal information, we agree with stakeholders who have raised concerns about the meaning of 'consent' in the context. The potential Privacy Act reforms recognise that consent needs to be voluntary, informed, current, specific and unambiguous in order to be considered as valid. The Bill and Rules, as currently drafted, do not articulate these requirements. We therefore consider that **Risk 2** (see paragraph 3.7 in **Part A [Executive Summary]**) exists in relation to the current drafting of the Bill and Rules, as there may be different approaches taken by accredited entities when seeking express consent. In the absence of any further wording changes to the Bill, we consider that **Recommendation 3** will assist entities to obtain valid consent from individuals by providing appropriate guidance about the elements that should be satisfied when obtaining consent. The Bill does not prohibit the collection of all sensitive information under the Privacy Act, but rather the 'intentional' collection of prohibited attributes. Again, as stakeholders have raised this may not fully capture the policy intent behind cl 41 (which we understand is to recognise that in

relation to the retention of the biometric information, and the discussion in APP 6 for the use and disclosure of biometric information). The Accreditation Rules provide that an accredited entity must only collect personal information in connection with its accredited services that is reasonably necessary for it to provide its accredited services (r 4.38). This is an important implementation of the 'data minimisation principle'.	some circumstances it may be unavoidable to collect a prohibited attribute, for example, if a person's photograph could disclose their religious belief). Again, without further guidance it may be difficult to determine when an entity has acted 'intentionally'. Again, in the absence of changes to the Bill to clarify, **Recommendation 3** could be used to assist in addressing this issue.

Principles behind APP 4 - Dealing with unsolicited personal information	
APP 4 is intended to ensure appropriate handling of personal information that an entity receives, but does not actively seek to receive (known as 'unsolicited information'). The intention is that, in most cases, if the entity could not have validly collected that information under the Privacy Act, it should not be permitted to keep that personal information (and if the entity is permitted to keep the unsolicited information, it should do so in compliance with its usual privacy requirements).	
Potential privacy risks and impacts if these principles are not implemented for the Digital ID System • Not having in place procedures to handle unsolicited personal information can lead to inappropriate handling and/or unauthorised disclosure of that information.	
Current measures in the Bill and Rules	**Potential further steps**
We do not consider it likely that individuals will provide unsolicited personal information to accredited entities in the context of the accredited services. However, if accredited entities do receive unsolicited personal information, the measures relating to the application of the APPs will mean entities will need to have relevant processes in place to appropriately manage any such information.	We do not consider that any further steps are required to meet the privacy principles behind APP 4.

Principles behind APP 5 - Notification of the collection of personal information

APP 5 is intended to ensure that individuals who have their personal information collected are notified about that collection, or are otherwise aware requires an entity that collects personal information about an individual to take reasonable steps to notify the individual of certain matters (referred to as "APP 5 matters"), or otherwise ensure that the individual is aware of those matters.

Potential privacy risks and impacts if these principles are not implemented for the Digital ID System

- Poorly drafted collection notices can undermine an individual's understanding of how their personal information will be handled.

Current measures in the Bill and Rules	Potential further steps
We consider the best practice privacy measures built into the Bill, particularly the requirements for public-facing information about how entities handle personal information in connection with the Digital ID System, will assist in ensuring that individuals are appropriately aware of relevant matters.	As part of its response to the Privacy Act Reforms report, the Government has agreed that privacy notices should be clear, up-to-date, concise and understandable, with appropriate accessibility measures in place (*Proposal 10.1*). The intention is for standardised templates for privacy policies and privacy notices to be developed for voluntary adoption by entities. While we do not consider anything further needs to be included in the Bill or Rules in relation to address APP 5 in particular, we consider that if **Recommendation 3** is implemented, OAIC could provide further guidance on this ahead of any Privacy Act reforms being enacted.

APP 6 - Use and disclosure of personal information

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).

Potential privacy risks and impacts if these principles are not implemented for the Digital ID System

- Uses or discloses personal information which are not in line with the express wishes of an individual, can lead to significant negative impacts on an individual, such as, risk of identity theft (and consequential financial and other losses) and psychological harm.
- The Digital ID System requires that accredited entities obtain the consent of individuals to disclose personal information to other entities in certain circumstances. Where the Bill requires the consent of an individual for an entity to take certain action, there is a risk that individuals may not understand what they are being asked to consent to and entities may not be able to demonstrate that they have the valid express consent of individuals.

Current measures in the Bill and Rules	Potential further steps
The Bill includes a number of restrictions on the use and disclosure of personal information collected by an accredited entity, including: • the requirement in cl 42 of the Bill to obtain express consent of an individual to the disclosure of certain attributes (e.g., the individual's name, address, data of birth and phone number) to a relying party; • when verifying or authenticating an individual's identity, an accredited entity must not under cl 43 of the Bill send a restricted attribute of an individual (e.g., details of their passport or licence number) to a relying party unless: ○ authorised to do so by an accreditation condition; and ○ only with the individual's express consent; • restrictions under cl 44 of the Bill about when a unique identifier that has been assigned by an accredited entity can be disclosed by the entity. We note that there are exceptions where disclosure is permitted (exceptions include where it is necessary to detect fraud or a cybersecurity incident, or where the disclosure facilitates the person accessing a service using their Digital ID)[29],	The restrictions on the use and disclosure of particular attributes of individuals and biometric information under the Bill go some way to addressing the risks and impacts associated with the use and disclosure of personal information. As discussed above in relation to APP 3, the potential Privacy Act reforms recognise that consent should be voluntary, informed, current, specific and unambiguous (and that this should be defined in the Privacy Act). We consider that **Risk 2** (see paragraph 3.7 in **Part A [Executive Summary]**) exists in relation to the current drafting of the Bill and Rules, as there may be different approaches taken by accredited entities in seeking express consent. In the absence of any further wording changes to the Bill, we consider that **Recommendation 3** will assist entities to obtain valid consent from individuals by providing appropriate guidance on the elements that should be satisfied in obtaining consent. We support the inclusion of the provisions that require only minimum personal information to be disclosed to a relying party (Accreditation Rules, r 4.38). However, we are concerned that Rule 4.38(4) does not specify what steps an accredited entity must take before it discloses personal information to a relying party (i.e., to establish that the relying party reasonably needs that information). The rule is not linked to the

[29] Bill, cl 44(4) and (5).

but from a privacy perspective those exceptions seem reasonable; and • restrictions on using or disclosing biometric information (which are the same as those discussed in APP 3 above, and in paragraph 11 in this **Part C** above); We particularly support the restrictions on disclosing biometric information to a law enforcement agency, which are limited to situations where a warrant has been issued (meaning that the need for the disclosure will have been subject to objective scrutiny from a body other than the law enforcement agency seeking to obtain that information) or the consent of the individual has been obtained (see Bill, cl 46(3)). We do note the allowance for the use of biometric information for testing in relation to the information by an accredited identity service provider (Bill, cl 46(6)-(7), but this is subject to a range of additional protections, including the detailed requirements specified in the Accreditation Rules; • 'data profiling' to track online behaviour is prohibited, except in limited situations (which from a privacy perspective appear to be reasonable) (Bill, cl 50); • use or disclosure of personal information for law enforcement purposes is limited to specified situations (which from a privacy perspective appear to be reasonable) (Bill, cl 51); and • use or disclosure of personal information to undertake testing in relation to the AGDIS is permitted, but must be specifically authorised by the Digital ID Regulator (Bill, cl 77 and 78). (See also use and disclosure of personal information for marketing purposes discussed in APP 7 below). The Accreditation Rules also contain some important protections for the disclosure of personal information by accredited entities. Rule 4.38(2) effectively provides that such an entity can only disclose personal information to a relying party if it is satisfied that the relying party reasonably needs that information to provide its service to the individual or allow them to access their service. The Accreditation Rules clarify that an accredited entity can satisfy this requirement by having processes in place	taking of 'reasonable steps', as defined in rule 1.6, so it is unclear if it would be sufficient if the relying party has simply represented that it does require the particular personal information. In these circumstances, we consider that it would be appropriate for clear guidance to be provided by the Information Commissioner (see **Recommendation 3**).

to verify that the personal information sought by the relying party is reasonably necessary for their activities (Rule 4.38(2)). Finally, it is important to recognise that the uses and disclosures that accredited entities may wish to undertake in connection with Digital IDs are likely to change over time. In this regard, we support the inclusion of a mandatory review of the operation of the Act within the first 2 years of operation (Bill, cl 153). In our view, this will allow consideration of whether the protections in the Bill and Rules remain in line with community expectations, or whether additional privacy protections should be included.	

Principles behind APP 7 - Direct marketing	
APP 7 in intended to ensure that entities which are 'organisations' under the Privacy Act (and "agencies" only in limited circumstances) are generally not permitted to not use or disclose personal information for the purpose of direct marketing (unless an exception applies, for example because they are contracted to an agency to provide direct marketing services).	
Potential privacy risks and impacts if these principles are not implemented for the Digital ID System • Individuals may receive unwanted communications where they have not authorised, or would not reasonably expect this use of their personal information.	
Current measures in the Bill and Rules	**Potential further steps**
Clause 52 of the Bill prohibits accredited entities from using or disclosing an individual's personal information for marketing purposes that are unrelated to the Digital ID services the entity provides to the individual.	We do not consider that any further steps are required to meet the privacy principles behind APP 7, other than potentially further clarifying what is services are intended to be 'related' to Digital ID services (so that 'unrelated' services can be clarified (see **Risk 2** and **Recommendation 3**).

Principles behind 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.	
Potential privacy risks and impacts if these principles are not implemented for the Digital ID System • 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.	
Current measures in the Bill and Rules	**Potential further steps**
The Bill at cl 73 does not prohibit the holding, storing, handling or transfer of information outside of Australia by accredited entities, rather it provides that this issue can be addressed in the Digital ID Rules. Rule 10 of the Digital ID Rules generally provides that an accredited entity must not hold, store or handle personal information collected or generated through the AGDIS outside of Australia. Rule 10 does provide a process for entities to seek an exemption from the Minister from this 'data localisation' rule, including the ability to take into account a PIA provided by the entity, and the effectiveness of the entity's protective security and fraud control arrangements. The Minister must be satisfied of certain things prior to granting any exemption, including that the place outside of Australia where the data will be held has protections substantially similar to the APPs. Further Accreditation Rules require entities seeking accreditation to submit a copy of a PIA conducted in respect of their Digital ID data environment and proposed accredited services (Accreditation Rule, r 2.2(1)(j). This will necessarily require consideration of whether any personal information will be held or disclosed outside of Australia, and its compliance with the requirements of APP 8.	We do recognise that there may be limited circumstances where it may be appropriate that the data localisation rule does 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 consider that r 10 of the Digital ID Rules provides a robust 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. Therefore, no further steps are proposed to in respect of the principles behind APP 8.

Principles behind APP 9 - Government related identifiers

APP 9 is intended to ensure that identifiers issued by or on behalf of governments are not adopted by organisations as their own identifier for the individual, and that their use and disclosure of those identifiers is restricted to particular situations where it is considered appropriate.

Potential privacy risks and impacts if these principles are not implemented for the Digital ID System

- Failure to comply with this principle raises concerns about the implementation of an 'Australia Card', with associated concerns about the monitoring and tracking of individuals.

Current measures in the Bill and Rules	Potential further steps
Government identifiers (issued or assigned by the Commonwealth, State or Territory entities) are 'restricted attributes' (see cl 11(1)(b) of the Bill). Under cl 43 of the Bill, an accredited entity must not disclose a restricted attribute of an individual to a relying party unless: • authorised to do so by an accreditation condition; and • only with the individual's express consent.	We consider the Bill overrides the operation of APP 9 in the context of accredited services, but nevertheless meets the principle behind APP 9. Again, as discussed in relation to APP 3, it will be important to ensure that consent obtained from individuals by accredited entities is valid. We consider that **Recommendation 3** will assist in addressing **Risk 2** by providing appropriate guidance on the elements that should be satisfied when obtaining consent.

Principles behind APP 10 - Quality of personal information

APP 10 is intended to ensure that entities take reasonable steps to ensure that the personal information that they collect is accurate, up-to-date and complete, and that they take reasonable steps to ensure that they only use or disclose personal information meets these requirements and is also relevant, having regard to the purpose of the use or disclosure.

Potential privacy risks and impacts if these principles are not implemented for the Digital ID System

- Handling poor quality personal information could mean that the individual is not able to obtain a service, or that a person obtains a service which they should not.

Current measures in the Bill and Rules	Potential further steps
The Accreditation Rules contain detailed technical standards which will assist to ensure that high quality data flows through the entities participating in the Digital ID System. We particularly note the requirements for testing of biometric information (including for system demographic bias).	No further steps are proposed in respect of APP 10.

Principles behind APP 11 - Security of personal information

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.

Potential privacy risks and impacts if these principles are not implemented for the Digital ID System

- If personal information is not secured and well protected, it could lead to data breaches, resulting in significant harm being caused to affected individuals.

Current measures in the Bill and Rules	Potential further steps
An entity's ability to appropriately protect personal information that it holds is a matter that is relevant to the Digital ID Regulator's decision about whether or not to accredit that entity (Bill, cl 15(4) and (5); cl 16). Accreditation is subject to conditions, which can include a condition imposed for reasons of security (Bill, cl 18). Approval to participate in the AGDIS is also subject to conditions, including those relating to security (Bill, cl 62). The Bill also gives the Digital ID Regulator the power to suspend or revoke accreditation (so that the entity will not be able to continue to provide Digital ID services) or approval to participate in the ADGIS (so that the entity will no longer be able to participate) if there are particular security concerns (Bill, cl 24- 26; cl 60 and 68-70). The Bill and Rules also include a range of measures for accredited entities which are designed to provide a very high level of protection to personal information. These include, for example, requiring accredited entities to: • undertake assurance assessments and systems testing, both on application and on an annual basis (Accreditation Rules at Chapter 3). For example, a protective security assessment is required, as is penetration testing; • implement and comply with specified information technology system controls, including that all Digital ID information must be protected in transit and at rest by approved cryptography (Accreditation Rules, r 4.17 -21)	We consider that the Bill and Rules will establish a robust framework to manage the security risks associated with the Digital ID System, but that a further reasonable step that could be taken is reporting on the implementation of PIAs conducted by entities (see **Risk 3** and **Recommendation 5**). As with the issue about whether State and Territory laws are 'comparable' there is also an issue in relation to whether a data breach notification scheme under a State or Territory law is 'comparable' to that in Part IIIC of the Privacy Act. For example, although the scheme that will commence under the *Privacy and Personal Information Protection Act 1998* (NSW) has been closely modelled on that in the Privacy Act, over time the NSW and Commonwealth Parliaments may implement differences to those Act, as they further consider and refine their requirements. We consider that **Recommendation 3** will assist in address **Risk 2**, by ensuring that all participating entities are aware of their data breach reporting obligations.

• undertake cyber security risk assessments, and incident monitoring and reporting (e.g., Accreditation Rules, r 4.13 – 4.14); • provide annual reporting (Accreditation Rules); • participate in any compliance assessments undertaken by the Digital ID Regulator (Bill, cl 126-127); • provide advice to individuals about how to safeguard their Digital ID against cyber security risks (Accreditation Rules, r 4.8); • have a cloud services management plan, which must include particular strategies designed to reduce cyber security and other risks associated with the use of cloud services; (Accreditation Rules, r 4.12); and • implement non-technical measures, such as privacy awareness training of personnel (e.g., Accreditation Rules, r 4.40). There are additional requirements for entities participating in the AGDIS to report matters to the Digital ID Regulator if they occur, such as of cyber security incidents and digital ID fraud (Digital ID Rules, r 12 and 13), so that they can be taken into account in decisions about continued accreditation (or suspension or revocation of accreditation). Accredited entities are required to have and maintain a data breach response plan (Accreditation Rules, r 4.41). If the accredited entity has reasonable grounds to believe an eligible data breach (as defined in the Privacy Act) has occurred, the Digital ID Regulator as well as the Information Commissioner or relevant State/Territory privacy regulator must be notified. As discussed in APP 1, the expansion of the notifiable data breach scheme in Part IIIC of the Privacy Act to accredited entities who would not otherwise be bound by that scheme, or by a comparable State or Territory scheme (see Bill, cl 37-39), is an important measure (including because entities who know they will need to notify individuals of any data breaches may be even further motivated to protect personal information that they hold). The Bill also provides provisions in relation to the destruction of biometric information, which are more stringent than those in APP 11.2 (Bill, cl 48 : also see paragraph 11 above). Similarly, accredited identity exchange	

providers must not retain attributes of individuals after the end of the authenticated session (Bill, cl 53(2)). The Bill contains express requirements for destruction or de-identification of personal information after an entity's accreditation or approval to participation in the AGDIS is revoked (Bill, cl 130). However, the operation of the Bill will also generally mean that the entity who is not participating in the AGDIS (but is accredited) will be under an obligation (either under the Privacy Act, under a comparable State or Territory law, or because of the APP-equivalent agreement) to comply with the destruction or de-identification requirements in APP 11.2 for personal information held in connection with provision of their Digital ID services.	

Principles behind APP 12 - Access to personal information and APP 13 – correction of personal information These APPs are intended to ensure that an individual can access personal information about them which is held by an entity, and to correct that information if they believe it is incorrect, except in limited circumstances.	
Potential privacy risks and impacts if these principles are not implemented for the Digital ID System • Lacking appropriate procedures for a person to access and correct their personal information, undermines the person's ability to control their personal information.	
How privacy risks and impacts are addressed in the Bill and Rules	**Potential further steps that can be taken to address**
All accredited entities will be subject to the Privacy Act, or a comparable State or Territory law, or an agreement to comply with the APPs, including APP 12 and 13. The Bill also requires accredited identity service providers to deactivate a person's Digital ID as soon as practicable after receiving the request (Bill, cl 28). Although this is not directly relevant to APP 13, it provides a 'self-help' mechanism if an individual believes that the information in or associated with a Digital ID is incorrect.	No further steps are proposed in respect of the principles behind APP 12 and 13.

Part D Glossary

Definitions	
ACAPS 2023	means the *Australian Community Attitudes to Privacy Survey 2023* conducted by OAIC.
ACCC	means the Australian Competition and Consumer Commission.
Accreditation Rules	means the exposure draft of the Digital ID Accreditation Rules 2024 released on 19 September 2023 and available at: https://www.digitalidentity.gov.au/have-your-say/2023-digital-id-bill-and-rules-submissions.
accredited entities	means the entities that can provide Digital ID services under the Bill, namely identity service providers, attribute service providers, and identity exchange bodies.
APP Code	means the *Privacy (Australian Government Agencies – Governance) APP Code 2017*.
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	means information associated with an individual, as defined in cl 10 of the Bill.
Bill	means the exposure draft of the Digital ID Bill 2023 released on 19 September 2023 and available at: https://www.digitalidentity.gov.au/have-your-say/2023-digital-id-bill-and-rules-submissions.
biometric information	has the same meaning as in cl 9 of the Bill (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).
Department	means the Australian Government Department of Finance.
Digital ID	has the same meaning as in cl 9 of the Bill (which is a distinct electronic representation of the individual that enables the individual to be sufficiently distinguished when interacting online with services).
Digital ID Regulator	means the independent regulatory under the Bill with oversight of the Digital ID System, who be the ACCC.
Digital ID Rules	means the exposure draft of the Digital ID Rules 2024 released on 19 September 2023 and available at: https://www.digitalidentity.gov.au/have-your-say/2023-digital-id-bill-and-rules-submissions.
Digital ID System	means the voluntary accreditation scheme for Digital ID providers and expansion of AGDIS provided for in the Bill.

Definitions	
Information Commissioner	means the person appointed under section 14 of the *Australian Information Commissioner Act 2010* (Cth) (see section 3A of that Act which will import that definition into the Bill).
OAIC	means the Office of the Australian Information Commissioner, established under the *Australian Information Commissioner Act 2010* (Cth).
personal information	depending on the context, has the meaning given in section 6 of the Privacy Act, or cl 9 of the Bill.
PIA	means this privacy impact assessment.
Privacy Act	means the *Privacy Act 1988* (Cth).
Privacy Governance Code	means the *Australian Government Agencies —Governance) APP Code 2017* or replacement.
prohibited attributes	means information that accredited entities are not permitted to intentionally collect under cl 41 of the Bill.
restricted attribute	has the same meaning as in cl 11 of the Bill. It includes information such a tax file numbers, Medicare numbers and health information.
Rules	means the Digital ID Rules and Accreditation Rules.
sensitive information	has the meaning given in section 6 of the Privacy Act.
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.

Attachment 1 Methodology and Assumptions

1. Our Methodology

1.1 This PIA has been conducted in accordance with the *Guide to undertaking privacy impact assessments* issued by the Office of the Australian Information Commissioner (**OAIC**), using the methodology in the table below.

Stage	Description of steps
1.	**Plan for the PIA:** We reviewed the exposure drafts of the Bill, the Digital ID Rules and the Accreditation Rules, as well as the guides to the legislation prepared by the Department. We also reviewed the previous PIAs which were conducted in connection with this project. We were provided a briefing by officers from the Department. We agreed the timing for undertaking the PIA, and the format for the PIA report.
2.	**Stakeholder consultation:** The Department conducted a public consultation on the Bill, Digital ID Rules and the Accreditation Rules in September and October 2023. Multiple discussions were also held with private sector entities, over 15 roundtables and two online webinars were held with representatives from industry peak body organisations and community groups, including across: human rights; inclusion, legal, small and large businesses, banking and payments, consumer advocates and privacy and cyber security advocates. The Department received 113 submissions and 1,346 individuals participated in the online survey. The Department then provided us with a summary of those parts of those submissions which were relevant to privacy matters. We took this feedback into account, as well as our experience and knowledge of other relevant research (including the *Australian Community Attitudes to Privacy Survey 2023*, which provides useful and current information about the Australian community's attitudes to the handling of personal information by governmental and other entities), to inform the PIA.
3.	**Project Description**: We prepared a Project Description, which described the legislative framework at a high level. This description was refined in consultation with the Department, to ensure it accurately reflected the project.
4.	**Privacy impact analysis and compliance check**: In parallel with Step 3, we considered the Bill and Rules against the principles behind each APP and privacy best practice. In undertaking our analysis, we considered and applied the *Australian Privacy Principles guidelines* (**APP Guidelines**) issued by the OAIC, which outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters that may be taken into account when assessing compliance with the Privacy Act.
5.	**Privacy management and addressing risks:** Where we identified a privacy risk that had not been mitigated, or where there may be some uncertainty around the implementation of the proposed mitigation, we considered whether there may be further steps that could be taken to reduce or remove the privacy impacts and risks identified during the previous step, and developed our recommendations.
6.	**Draft report:** We prepared a draft version of this PIA report.
7.	**Further refinement of draft PIA report**: Following review of the draft report by the Department, we further refined our analysis and potential mitigation strategies as required to ensure that privacy risks and the intended mitigation strategies were appropriately considered, explained and addressed.
8.	**Final report**: We finalised this PIA report.

1.2 We understand that the Department will consider and provide its response to the recommendations in this PIA report, in a separate document.

2. Assumptions and Qualifications

2.1 We have conducted our analysis using the exposure drafts of the Bill, Digital ID Rules and Accreditation Rules as at 19 September 2023. We have not considered any further refinement of those drafts after this date.

2.2 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. As discussed in **Part A [Executive Summary]**, 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.[30]