ACT Government

ACT Government Submission 2023 National Consultation on the Digital ID Bill and Associated Rules

OFFICIAL

Australia's 2023 National Consultation on the Digital ID Bill and Associated Rules

Australian Capital Territory Government Submission

Introduction

This ACT Government submission details the ACT's comments, questions, and recommendations on the proposed exposure draft of the Commonwealth Digital ID Bill 2023, Digital ID Rules 2024 and Digital ID Accreditation Rules 2024.

Response Summary

The ACT Government supports the objectives of the proposed draft Commonwealth Digital Identity (ID) legislation to promote privacy and security of personal information, convenience in accessing services, and facilitate economic advancement through use of Digital IDs for consumers and business users, service providers, government, and the broader economy.

We also understand the need for a strong, secure, and well-regulated whole of economy Digital Identity System that facilitates choice and control for the individual in the creation and use of their Digital ID.

It is also acknowledged that Digital ID is one of the highest priorities for Data and Digital Ministers, however, we hold some reservations regarding some aspects of the proposed draft legislation, including:

- *Voluntary and Inclusive* – digital literacy, accessibility and inclusive design, for both the user and participating entities, and variation in the practical application across entities will affect the user experience;
- *Interdependencies* – with other biometric initiatives and other Commonwealth, State and Territory legislation especially for voluntary use and for law enforcement;
- *Ministerial Powers and Standards* – ensuring risk of unintended consequences of rulemaking is appropriately assessed and managed including the need to consider various models to ensure it is best suited to proposed voluntary scheme;
- *Charging framework* – fee structure and application including impacts on citizens, accredited and participating entities in the system is yet to be determined;
- *Legislative Consistency and Alignment* – with the ACT's Privacy and Human Rights legislation and *Security of Critical Infrastructure Act 2018* (Cth); and
- *Technical Matters and Capability Uplift* – understanding the technical and other capabilities required for participating entities, data ethics and work required (including financial impacts) for a small jurisdiction such as the ACT.

Further to submission, please find attached the ACT Government's response to the Guide Questions proposed as part of the consultation process at Appendices Appx A - Digital ID Bill and Rule and Appx B - Digital ID Accreditation Rules.

Key issues

We have identified the following key issues the proposed draft Commonwealth Digital ID legislation and associated rules may present for the ACT Government, our citizens and residents, both to our current and potential future states in respect to voluntary participation and/or accreditation in the Australian Government Digital ID System (AGDIS).

We note that these issues may not solely be of concern to the ACT Government and may be of significance to business and other entities in the private sector. We strongly encourage the Australian Government, when drafting the final legislation, scope and timing of the proposed four phases of implementation, to consider the following with the interests of all potential users and participant of the AGDIS.

Voluntary and Inclusive

Voluntariness and verifiable credentials

We recognise some users may find meeting the Proofing Guidelines for verifiable credentials, including some proofing levels, for the creation and use of a Digital ID challenging or prohibitive due to the particular characteristics of certain populations e.g., those members of our community who may not have been registered at birth or whom have been in transit arrangements for a significant period of time.

Key concern: If the Proofing Guidelines and levels do not accommodate for an equivalency, agreed across jurisdictions, allowing for specific circumstances for certain individuals or groups, then these people will be further disadvantaged as they already face significant barriers to participating in the digital economy or accessing certain digital services or information.

Inclusive design, digital literacy and accessibility

Ongoing consultation with marginalised groups and users is vital to ensuring an inclusive approach to establishing a whole-of-economy Digital ID and governments need to actively seek to not exclude certain segments of our community. We understand the Australian Government continues to undertake research and consultation with a range of community and interest groups such as those representing First Nations, persons living with disability, those whom are experiencing homelessness, rough sleepers, youth requiring access to mainstream services (from the age of 14) and persons with English as a Second Language and Culturally and Linguistically Diverse (CALD) groups to name a few. This work needs to remain ongoing to inform implementation and any periodic reviews of Digital ID legislation, if passed.

Key concern: The ACT would like to see insights arising from the more recent work commissioned by the Australian Government on inclusion and uplift of digital literacy and accessibility to inform the proposed draft legislation, any further national and local consultation and supporting communications with the community on the proposed Digital ID legislation, if or when passed.

Interdependencies

Associated biometric initiatives

We are aware of several other current biometric initiatives that this proposed draft Digital ID legislation may impact, or be impacted by, such as the Identity Verification Services Bill 2023 (IVS Bill) in regard to underpinning Facial Verification Services (FVS) and the Document Verification Service (DVS), which will establish legislative authority over the National Drivers Licence and Facial Recognition Solution (NDLFRS) that road transport authorities may be contributing too.

We advise that constraints specific to the ACT that were required to be reflected before signing the Inter-Governmental Agreement (IGA) for FVS in 2017 are as follows:

- Access to the ACT's data for FVS will be for limited purposes listed in clause 1.2 of the IGA (preventing identity crime, general law enforcement, national security, protective security, community safety and identity verification),
- Access to the ACT's data via FVS will only be for the purposes of national security and community safety; and
- The ACT will not participate in One Person One Licence Service (OPOLS) - a limited one-to-many search to detect instances where a person holds multiple driver licences across jurisdictions.

As a result of these constraints, the ACT is yet to contribute any biometric images to the FVS.

Key concern: The ACT's ability to participate or be accredited in the voluntary scheme outlined in the proposed draft Digital ID legislation may be dependent on reform to ACT legislation, and Hosting and Participation Agreements associated with identified biometric initiatives.

Voluntary use and law enforcement

We agree the need for strong penalties that may assist in the protection of privacy by deterring any unauthorised handling of personal information, attributes associated with an individual, or their Digital ID itself by any entity.

Key concern: The ACT is not currently satisfied there is a shared understanding and alignment between the Commonwealth and State and Territories about key sections of the proposed draft Digital ID legislation and rules of relevance to exceptions for disclosure for voluntary use, or for law enforcement.

We also understand NSW is progressing their own Digital ID legislation currently. As the ACT has a very close relationship with NSW, and given the fluidity of movement across our borders, there is a requirement for alignment of legislative frameworks or processes applied across jurisdictions to ensure consistency of community expectation about how their information and credentials will be handled by participating tiers of government. In particular, consideration must be shown to matters such as disclosure for law enforcement, disaster or emergency response.

Ministers Powers and Standards Model

Rulemaking - Disclosure

The rulemaking power allows for the disclosure of an attribute prescribed by the Digital ID Accreditation Rules (this may include biometric information or restricted attributes) by accredited entities under specified circumstances. The responsible Commonwealth Minister for AGDIS, when making a Rule is required to consult with the Office of the Australian Information Commissioner (OIAC) and to consider certain matters including: general expectations of the community, if any harm to the community may result or if the disclosure may be governed by another law of the Commonwealth. The proposed draft Digital ID Bill is silent, however, on the matter where there could be potential unintended consequences or conflict with State or Territory legislation (such as the *Births Deaths Marriages Act 1997* (ACT)) that may impose restrictions on the disclosure of source verification of that attribute or credential.

Key concern: The ACT has a broad range of legislation governing personal information, personal identifiers, and other types of personal information that may be consumed by the Digital ID ecosystem. Some of this personal information is also subject to prohibitions on its disclosure. If adequate consideration is not given to how any new or proposed Accreditation Rules may apply, this may limit the ACT's ability to participate or be accredited in the AGDIS as outlined in the draft legislation.

Recommendation: The responsible Commonwealth Minister when making a new Accreditation Rule under the proposed draft Digital ID legislation should be required to consult States and Territories to confirm what (if any) prohibitions there are on disclosure, or if that information is otherwise further regulated, under local legislation.

Rulemaking – Recovery of a Digital ID

Noting the differences in the ability of State and Territory capacity to provide proofing to the same standard, in the case of natural disasters, local governments are often the first point of contact for their affected residents, however we note local governments are outside the scope of this legislation.

Opportunity: Noting the benefits Digital IDs can bring to individuals and businesses, there is an opportunity to extend the scope of the Commonwealth Minister's powers to a limited pre-approval of local government or other auxiliary to Government private entities such as the Australian Red Cross, during disaster and/or emergency response or recovery period as a Relying Party. These community recovery functions would be in addition to any immediate services offered by the Australian Government.

Consideration of this arrangement holds potential to streamline recovery response enabling individuals and business representatives streamlined access to necessary services (including payments, financial support and services offered by private enterprise such as insurers, banks, telecommunications providers etc) in the days and weeks following a disaster. This would also support the principles of the National Strategy for Identity Resilience recently agreed to by the Commonwealth and all States and Territories.

Standards Model

We understand the Standards model to be applied, is still under consideration. While adoption of the Consumer Data Right model is proposed, we understand the Australian Government may be open to alternatives.

Recommendation: We would encourage the Australian Government to consider alternative models with each option to be assessed on their merits with learnings reflected from recent models used for other legislation with like requirements. There may an opportunity to leverage work already underway in States and Territories.

Charging framework

Noting a charging framework and fee structure has yet to be determined, it is acknowledged the proposed draft Digital ID legislation states fees must not be charged to an individual for the creation or use of their Digital ID, and fees may be deemed by the Digital ID Regulator as nil.

It is the ACT Government's view (as previously communicated):

- the fundamental value of digital ID has a significant positive impact on the growth of the national economy. The cost of administering the central (and critical) infrastructure to support AGDIS should be the responsibility of the Commonwealth (as recommended in the recent myGov audit), particularly given the value in ensuring all States and Territories participate in the AGDIS, and all jurisdictions have invested in their own identity systems to date;
- the ACT does not agree with State and Territory Government's being charged to consume services as a Relying Party given jurisdictions are part of the identity ecosystem that creates the trust chain and charging would be a barrier to participating in the AGDIS, putting at risk the success of a national system;
- the ACT does not agree with the principle of commercialising the proofing and authentication of citizen identity given the identity itself is something that belongs to the citizen; and
- if the private sector is given the opportunity to be accredited or participate in the AGIDS in Phase 4 or earlier, then charging these entities for the service may be appropriate and reasonable but must consider the indirect impacts of fees being passed onto others as per the current fee arrangements for American Express.

Recommendation: Noting a framework and fee structure in the proposed draft Digital ID legislation is yet to be determined, or agreed with States and Territories, raises concerns for the ACT Government (as an identity provider and relying party), residents, businesses and other entities operating in the Territory as we are unable to undertake the appropriate analysis to understand impacts.

The ACT Government recommends the cost of the entire Digital ID System, from the creation of the identity documents to the retiring of an identity and impacts on the broader community, be determined in the first instance before any charging framework or fees are set, noting States and Territories already contribute significantly to supporting the cost of the identity system.

Legislative consistency and alignment

Critical Infrastructure

The ACT Government's recent response to the Australia's National 2023-2030 Australian Cyber Security Strategy Discussion Paper highlighted the need for Digital Identity as an asset to be protected and secured against malicious actors and cyber-attacks. It further recommended key parts of the broader Australian Digital Ecosystem should be considered national assets and be protected such as: Identity Providers (those systems that manage user identity verification); attribute, credential and relationship providers; and sources of truth for documentation used to verify an identity e.g. (DVS, FVS, State and Territory based licences, and Births, Deaths and Marriage registries). This would likely include the Digital ID System including AGDIS.

Key concern: In the event the *Security of Critical Infrastructure Act 2018* (Cth) is amended to include 'information assets' and Digital ID System (in part or full), any future amendments required to the proposed draft Digital ID Bill including associated Rules will need to consider the risk of unintended consequences and additional regulatory burdens for entities, which may delay proposed implementation of the voluntary accreditation scheme and expansion of the AGDIS.

Privacy

There are inconsistencies with the draft legislation and the *Information Privacy Act 2014* (ACT), in regard the following matters:

Mandatory Breach Notification

The ACT is in a unique position regarding the OAIC as the Regulator for privacy-related matters in the proposed draft Digital ID legislation, as the Commonwealth Privacy Commissioner is appointed as the ACT Information Commissioner by the Executive under an Agreement. The proposed draft Digital ID legislation provides for non-Australian Privacy Principles (APP) entities under an Agreement, comply with the *Privacy Act 1988* (Cth) where they do not have adequate or similar State or Territory legislation.

While the ACT Government acknowledges a requirement for mandatory breach reporting, in alignment with the National Data Breach Scheme or State or Territory equivalents, the ACT does not have equivalent mandatory breach reporting obligations under the *Information Privacy Act 2014* (ACT).

Key concern: Due to the limited time for consultation on the proposed draft Digital ID legislation, the ACT needs more time to understand if differences in the ACT's privacy legislation represents a significant barrier to participation or accreditation (if sought) in the AGDIS. The proposed draft Digital ID Bill in its current form may limit the ability for the ACT to participate or seek accreditation due to mandatory breach notification requirements, which do not currently apply under the Territory's privacy legislation. If s38(3) and s38(4) of the proposed draft Digital ID Bill are unable to be flexibly applied, then the ACT will need to obtain appropriate advice on the matter to understand what (if any) adjustments or amendments to ACT legislation might be required to meet s39 of the proposed draft Digital ID Bill.

Minors and consent

We understand the proposed draft Digital ID legislation has determined the minimum age a minor or young person may create and use a Digital ID is 15 years of age. This is based on the OAIC APP Guidelines on consent and minors, where the *Privacy Act 1988* (Cth) itself does not specify an age for consent. The *Information Privacy Act 2014* (ACT) similarly does not specify an age for consent. Both Act's rely on the principle that, in general, someone of 18 years of age is capable of consent and is assessed on a case-by-case basis. Where that is not practicable, it may be presumed that a young person 15 years or older may be mature enough to provide consent.

It is noted in the proposed draft Digital ID Accreditation Rules that during consultation, consideration may be given to lowering the age from 15 years to 14 years. This, we understand, is to align with community expectations and other important services for which young people may use a Digital ID, for example, when seeking a Tax File Number (TFN), applying for a Medicare Card, or using My Health Record, which permit a young person of 14 years of age to have their own record.

Key concern: While ACT agrees in principle, we would require further time to consult to determine if there were other matters across ACT Government, where minors and young persons might be impacted such as in relation to Human Rights, and to gain consensus with other States and Territories colleagues regarding an agreed age.

Express Consent

We support the need for 'express consent' by individuals to the disclosure of certain 'attributes' to Relying Parties as described in the proposed draft Digital ID legislation. However, while 'consent' is defined in both the *Privacy Act* 1988 (Cth) and the *Information Privacy Act* 2014 (ACT), neither of these Acts provide further guidance as to what is required for satisfactory 'consent'.

Key concern: The Digital ID Bill provides no further guidance on what is expected of 'express consent', so may be interpretated and applied inconsistently between Commonwealth and State and Territory entities, which raises risks associated with an 'invalid' consent for all participating agencies.

Recommendation: For consistency, ACT Government strongly encourages the development of advice aligned with available OAIC Guidance dealing with 'express consent'.

Consent for third parties to act such as Legal Business representatives or Enduring Power of Attorney (EPOA)

In respect of Legal and Business representatives, the ability to already transact in the AGDIS on behalf of a business is available currently. Over time it is expected the Relationship Authorisation Manager (RAM) for business to government interactions will be expanded.

In respect of EPOA, it is acknowledged the Australian Government is working with other government agencies, individuals, and private sector entities to determine whether one or many solutions to support EPOA are needed and this work remains ongoing.

Key concerns: The ACT Government suggests the outcomes of the work undertaken by Attorney-General and State and Territory counterparts in 2021 seeking to align EPOA provisions across all jurisdictions be considered in the proposed draft Digital ID legislation. These outcomes would also assist States and Territories in considering EPOA requirements in our own jurisdiction and what (if any) legislative amendment or other supports might be required to be accredited or participate in the AGDIS.

Deactivation of digital identities

Deactivation is not defined in the Digital ID Bill, and it is unclear if handling of requests for 'deactivation' of Digital Identities is a purely administrative matter or may at times be considered a privacy matter by individual users.

Requests for amendment, change, or deletion of personal information are currently commonly dealt with as requests for 'correction' under the *Privacy Act 1988* (Cth) and the *Information Privacy Act 2014* (ACT). Both have statutory timeframes of 30 days for responding to requests. It is also generally sound administrative practice when responding to requests from end users in respect of information held by an entity, to set expectations on how such requests will be handled, including timeframes for service.

Without clear setting of end user expectations relevant to response timeframes when deactivating their account (in alignment with either the Privacy Act or if specified in the proposed draft Digital ID Bill), they may make complaints to the Regulators. This then raises the question of which Regulator should or ought to handle such complaints, ACCC or OAIC.

We note that having any timeframes for a response buried in subordinate policy or standards is not in keeping with the Privacy Commissioner's views regarding aligning and not layering privacy regulation of the program. In most cases, ACT Government information or Australian Government information is also subject to IPP or APP 13 (respectively) regarding statutory record keeping requirements, and that currently there is no 'right to be forgotten'.

Key concern: Having no statutory timeframe for deactivation requests represents a potential source of complaints and referral to Regulators through inconsistent handling across jurisdictions or providers. There is an opportunity to make clear the definition, applicable standards for complaint management and resolution, and escalation process for end users.

Deceased persons

It is unclear how Digital IDs associated with deceased persons are to be managed, and how the operation of the proposed draft Digital ID Bill, where certain attributes and biometric information gives additional protections, may create a circumstance in which deceased person's information may not be accessible, or otherwise able to be deactivated upon request from a family member or an executor of their estate.

Key concern: ACT Government seeks more clarity on relevant definitions to understand the grounds for interpretation and in what circumstances a deceased person's Digital ID may be accessed, used, disclosed or deactivated.

Technical Matters and Capability Uplift

Technical vs Regulatory oversight

The proposed draft Digital ID legislation proposes two Regulators – Australian Competition and Consumer Commission (ACCC) and Commonwealth Information Commissioner, with Services Australia as administrator of AGDIS and a Standards Chair (to be appointed by the responsible Commonwealth Minister). However, it is unclear who has oversight of the AGDIS. We understand a 'collaborative approach' has been taken among a number of Commonwealth agencies and entities including Department of Finance and Australian Taxation Office in addition to the above stated roles.

Key concern: While comfortable with the regulation of accreditation and privacy-related matters under the proposed draft Digital ID legislation, arrangements for the regulation of the AGDIS itself is unclear. The proposed 'collaborative approach' rests on internally agreed governance and policies of current agencies and entities. Without that agreement being formalised in a transparent manner, there is a risk that over time those governance arrangements will break down or be lost during future (and eventual) machinery of government changes thus creating uncertainty for accredited or participating entities and undermining potential success of a national system.

Artificial Intelligence and Automated Decision Making

ACT Government believes that while the proposed draft Digital ID legislation is intended to be technology agnostic some emerging issues such as Artificial Intelligence (AI) should be given some consideration, in particular the issue of Automated Decision Making (ADM) when using the end output of a Digital ID ecosystem. This is not regarding the proposed technical testing permitted under the Digital ID Rules and Digital ID Accreditation Rules, but rather the implications more broadly for Relying Parties and the end users.

While the ACT understands accredited entities may face no liability for any results based on the Digital ID exchanged (having met all underpinning requirements and meeting all operational guidance and rules) there are some fundamental issues regarding the use of AI in ADM. We would contend some level of assurance or human oversight in the form of intermittent testing regarding the 'ID' itself should be undertaken where any ADM is used for an administrative outcome.

For example, in New Zealand their Privacy Commissioner has issued guidance on AI and their privacy principles, IPPs [1] noting that where AI is used in decision making, it should have human oversight applied.

We note the Digital Platform Regulators joint submission on AI[2] date 11 September 2023 to the OAIC, raised concerns and proposed opportunities for regulatory frameworks to strengthen positions and safeguards for the Australian public regarding AI. On 19 September 2023, the Hon Minister Katy Gallagher, Minister for Finance together with the Hon Ed Husic MP, Minister for Industry and Science, also advised an AI Taskforce will be stood up to guide work across the Australian Public Service.[3]

Key concern: While not specifically within the remit of the proposed draft Digital ID legislation, the ACT Government strongly encourages consideration of the uses of Digital ID in any ADM from a data ethics perspective, which may need to be considered within the scope of the Regulators to comment and/or encourage uplift in governance or oversight.

Capability Uplift

Currently one ACT Government business application in the ACT Revenue Office consumes myGovID for customer credentials. While we support additional secure ways for our citizens to access services, the ACT is yet to determine the way in which we will participate more broadly, and which specific technical model or standards may be applied and in what capacity such as an Attribute and Identity Provider, Relying Party or as an Exchange.

Key concern: ACT Government needs further time to consider the implications of accreditation for our current use case, and then to consider what it might look like to provide services at scale and uplift capability across ACT Government to participate in the AGDIS and support the needs of Australians. This would include the need to consider the technical, policy, and standards required for participation or accreditation (which may require significant investment to achieve) to meet the needs of our relatively small population. This concern was raised by other smaller jurisdictions at the recent Data and Digital Ministers Meeting on 29 September 2023.

In Conclusion

ACT Government would like to thank the Department of Finance Digital ID Taskforce for the opportunity to provide feedback on the proposed draft Digital ID legislation.

The ACT Government looks forward to collaborating further to resolve the matters raised with other States and Territory, and in being able to support and contribute further to this work as it is progressed.

[1] Office of the Privacy Commissioner | Artificial Intelligence and the IPPs
[2] Digital platform regulators make joint submission on AI | OAIC
[3] Digital ID and AI insights: How the Albanese Government is leading the digital evolution | Digital Identity

Key questions on the Digital ID legislation and Digital ID Rules

Page # of Guide	Question	Our Response
14	What other types of Digital ID service should be included in the legislation, either now or in future?	No comment.
14	Does the Minister's rule-making power to include new services over time provide appropriate flexibility to add new types of Digital ID services? If not, why not?	Ministers Power to make Rules, while providing some flexibility, is not best practice when considering controls when personal information is being handled. We agree with the OAIC's position, noted in their previous Digital Identity Legislation Position Paper on (15 July 2021), noting: *"The OAIC recommends that privacy requirements are embedded in the primary legislation to guard against inadvertent or unforeseen risks to privacy, such as the collection, use or disclosure of personal information that may not have been originally intended, known as 'function creep', or that which may not be reasonable, necessary and proportionate to the relevant policy objectives."*
16	Is the Regulator's power to impose conditions on accreditation an appropriate mechanism to balance the need to provide for unique characteristics of accredited entities with the need for a consistent set of Rules for the Accreditation Scheme? If not, how can the	No comment due to limited time to consider.

Page # of Guide	Question	Our Response
	Regulator's power to impose conditions on accreditation be improved?	
16	Is the application for accreditation process appropriate, or should other matters be included or some excluded?	No comment due to limited time to consider.
17	Are the maximum penalties for failure to meet accreditation requirements sufficient to deter accredited entities from not meeting their obligations? If not, what maximum penalties would be an appropriate deterrent?	Uncertain until this is tested however consideration should be given to the market value of the National Digital Identity System and costs to the impacted entities, both accredited and participating.
21	Are the additional privacy safeguards sufficiently robust, clear and practical?	There are inconsistencies, please refer to our attached submission paper for other notes. <u>Enforcement bodies</u> Suggest for permitted exceptions to disclosure to an 'enforcement body' be aligned to the OAIC's guidance on what is required for the *'making a note'* for both 'use' (internal to an entities own purposes) or 'disclosure' (external purposes) for an *'enforcement related function or activity'* on or behalf of an 'enforcement body'. The Annual Report requirements at S5.84 talks to the need for the maintaining of a 'record' which includes similar information required in APP6.5, but excludes the personal information: • S584(3)(c) *'but not so as to include the personal information of the individual'*,

Page # of Guide	Question	Our Response
		While an understandable privacy protection for the Annual Accreditation report, it is not practicable for the entity making the disclosure where often years later, enforcement bodies will return to request a witness statement in relation to the disclosure. This often proves difficult unless you have a register of all such disclosures in accordance with APP6.2(e), where APP6.5 requires the *'making of a note'*. Without the note, it may be all but impossible to supply a statement as to the information provided to the enforcement body, making or retendering their effort to progress a matter to court without 'confirmation' of the provenance of the information they collected inadmissible. In the Section 51 (1) they need to be 'satisfied' but there is no explanation of what that test might be? This while providing a prohibition on disclosure and an added protection, without guidance on what constitutes how one is 'satisfied' may end up open to wider interpretation defeating the purpose of the prohibition? If disclosing in accordance with S51(1), the disclosure will be then in accordance with APP6.2(b) '*where required or authorised by or under an Australian law, court or tribunal order*'. There are no requirements to make a note of the disclosure under the APPs (although its best administrative practice for the reason I have noted above), except for the Annual Reporting. Suggest should include the requirement to detail the following to align with the APP6.5 requirements for the making of a note; and APP6.2(e) of forming 'the reasonable belief' the disclosure is 'reasonably necessary', and which importantly requires the two-prong test to be satisfied.

Page # of Guide	Question	Our Response
21	Is the rule making power to allow disclosure of biometric information to enable sharing of verifiable credentials (under specified circumstances) an appropriate exception to the restriction on disclosure of biometric information?	Yes.
21	Is the maximum penalty for a breach of a privacy safeguard sufficient to deter accredited entities from interfering with a person's privacy? If not, what maximum penalty would be an appropriate deterrent?	Yes. However, we note the Governments response to the Privacy Act Review Report has been released, and it recommends new penalties for breaches. We would want to await any outcome of that report and any legislative amendment, before commenting further.
23	What is the appropriate age at which a young person should be able to create their Digital ID? What factors should be considered?	We agree lowering the age from 15 years to 14 years of age, to align with community standards and other service providers in alignment with other participants where relevant and agreed for consistency. Consideration should be given to the need for: • age-appropriate privacy noticing to ensure the consent meets the requirements for satisfactory consent; • whether the ID should also carry a warning that it belongs to a minor person and additional care should be taken when handling or storing the data; • the timeframe for 're-proof' the young person's credentials, should be reduced from 5 years to 2 years (or otherwise agreed) period given their continued development.

Page # of Guide	Question	Our Response
25	What other steps could the Government consider taking to ensure the AGDIS is ready for use by private sector relying parties and accredited entities?	Due to limited time provided during this consultation period we have been unable to consult with potential private sector entities in the ACT and recommend further consideration be given to this is done to determine what steps should be taken prior to seeking passage of the legislation in the Australian Parliament.
25	What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?	Further time is required to consider.
26	How would phasing the rollout of the ADGIS affect the wider Digital ID services market in Australia?	Further time is required to consider.
27	Is the balance between voluntary use and the exceptions to voluntary use right? Are any additional exceptions appropriate?	Refer to main submission.
27	Are the exemptions to the interoperability principle appropriate? Are any additional exemptions appropriate?	No comment due to limited time to consider.

Page # of Guide	Question	Our Response
29	Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?	No comment due to limited time to consider.
29	Are the protections for participants in the AGDIS appropriate, or are any additional protections needed?	No comment due to limited time to consider.
34	Noting the pace of technological change and the need for Digital IDs to stay protected by the latest developments, how can Data Standards provide an appropriate balance between certainty for accredited entities while maintaining currency?	No comment due to limited time to consider.
34	What would be an appropriate model for the Australian Digital ID Standards Chair and are there lessons that can be learned from the Consumer Data Right model?	The ACT needs more time to consider the proposed model.

Key questions on the Digital ID Accreditation Rules

Chapter 1 - free text response

Rule number	Page/Section/Topic	Our Response
1.4 - Definitions	Page 3 / Section 1.4 (1) / Definitions ***'data breach'*** means loss or misuse of, unauthorised access to, or unauthorised modification or disclosure of, personal information held by an accredited entity.	For consistency and alignment with the *Privacy Act 1988* (Cth) and Australian Privacy Principles (APPs), while this is a commonly cited definition of breach in contractual terms, MoUs or agreements, it is not the definition of a breach - it is the definition of what is expected regarding the security of personal information in APP11. The meaning of a breach is given in the Act at Sections 6A, 6B and in 6BA. In general, a breach is an act or practice that breaches and APP, and that may be broader than just the definition given regarding the 'security' of the personal information. This may include breaches about for example a Privacy Policy or Notice.

Chapter 2 - free text response

Rule number	Page/Section/Topic	Our Response
		No comment.

Chapter 3

Rule/Section	Guide Question	Our response
Chapter 3	1. Do you agree with the changes to the assurance assessments and kinds of systems testing required by the rules?	Yes, in principle.

Chapter 3	2. If you answered no to the above question, please provide your reasoning.	N/A
Chapter 3	3. Do you have any feedback or suggestions regarding the proposed rules in Chapter 3?	No.

Chapter 3 - free text response

Rule number	Page/Section/Topic	Our Response
3.4 Requirements	Page 14, S33.4(1)(a)(i)-(iii) Page 14	If there is an option for another model, other than ISO270001:2022 or the PSPF, would a hybrid be considered?
3.12 Usability Testing	S3.12(2)(a) and (b)	Requirement for user testing across a diverse range of individuals. Suggest the inclusion of the word 'cultural' as this is quite different to 'ethnicity' as 'ethnicity' does not always dictate 'culture'.

Chapter 4 - Protective Security

Rule/Section	Guide Question	Our response
4.10 and 4.29	4. Do you think the wording of 'likely to adversely affect individuals' in rules 4.10 and 4.29 is appropriate?	Yes – Suggest alignment with the concept of 'threshold of harm' or 'potential threshold of harm' with the *Privacy Act 1988* (Cth) and the NDBS to be able to apply before we considered the event to be *'likely to affect individuals'*. To be alert and not alarmed, is the desired affect and to notify or inform individuals of lower-level risk matters which are being effectively risk mitigated for, may produce a lack of trust, or create notification fatigue where genuine threat exists.

4.3	5. Do you agree with the 31 December 2024 timeframe for transitioning to ISO270001:2022?	No comment due to limited time to consider.
4.3	6. Are there any risks or issues with this transition timeframe?	No comment due to limited time to consider.
4.17 (and 3.5)	7. Do you agree with the implementation of the new Essential Eight requirements as currently drafted in the Accreditation Rules?	Yes, in principle, but need more time to consider.
4.17 (and 3.5)	8. If you answered no to the above question, please provide your reasoning.	N/A
4.17 (and 3.5)	9. Do you have any feedback or suggestions regarding the Essential Eight rules?	We note the only systems that require Maturity 2 are Federal Systems – while we appreciate the increased security what is the rationale behind Level 2?
Chapter 4, Part 1	10. Do you have any feedback regarding the proposed updates to the protective security rules?	No comment.

Chapter 4 - Protective Security free text response

Rule number	**Page/Section/Topic**	**Our Response**
		See note in Chapter 3 free text field on 3.4 Requirements – re hybrid option.

Chapter 4 - Fraud

Rule/Section	Guide Question	Our response
Chapter 4, Part 2	11. Do you agree to the change of policy relating to fraud?	Yes, in principle.
Chapter 4, Part 2	12. If you answered no to the above question, please provide your reasoning.	N/A
Chapter 4, Part 2	13. Do you have any feedback related to how this section of the Accreditation rules could better achieve its aim?	See free text notes below. Clarity around whether this can be an outsourced or delegated function would be useful.

Chapter 4 - Fraud free text response

Rule number	Page/Section/Topic	Our Response
4.22 Fraud Management Capability	Page 32, S4.22(1),(2),(3)Y	Forensic examination is a very specialised field, smaller jurisdictions and entities may not be able to provide this service in-house.
4.25 Fraud Controller	Page 33, S4.25 (1),(2),(3)	As above.

Chapter 4 - Privacy

Rule/Section	Guide Question	Our response
4.38	14. Do you agree that the data minimisation principle as drafted is able to satisfy the aims outlined above?	Yes.
4.38	15. If you answered no to the above question, please provide your reasoning.	N/A.
4.38	16. Are there any specific risks or issues with the rule as drafted?	Would suggest that the ***'reasonably necessary'*** be considered as there is no definition of this either in the draft legislation or in the *Privacy Act 1988* (Cth). This presents a risk for inconsistency across providers as to what is reasonably necessary for them. The concept of 'legitimate business' may prevail which while not dissimilar in the private sector in particular this may be rather 'bias', and have no basis in law that an Australian Government agency or other State/Territory agency may have by virtue of an identified function or activity that can point to or be demonstrated through: underpinning legislation, policy directives that are publicly announced, or other clearly defined reasons such as 'Budget portfolio statements', and Annual Reports etc.
4.38	17. What are your recommendations (if any) to improve the data minimisation principle?	***'Reasonably necessary'*** – as noted above, should be read in alignment with the OAIC's guidance on the APPs on same. OAIC APP Guidelines: B.107 The terms 'reasonable' and 'reasonably' are used in the Privacy Act and APPs to qualify a test or obligation. Examples include that 'personal information' is information about an individual

		who is 'reasonably' identifiable (s 6(1)) and an APP entity must not collect personal information unless it is 'reasonably necessary' for one or more of the entity's functions or activities (APP 3). B.108 'Reasonable' and 'reasonably' are not defined in the Privacy Act. The terms bear their ordinary meaning, as being based upon or according to reason and capable of sound explanation. What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. What is reasonable can be influenced by current standards and practices. B.109 The terms 'reasonable' and 'reasonably' are discussed further in the APP guidelines, as they arise in the context of each of the relevant APPs. It is the responsibility of an APP entity to be able to justify that its conduct was reasonable. In a related context, the High Court has observed that whether there are 'reasonable grounds' to support a course of action 'requires the existence of facts which are sufficient to [persuade] a reasonable person'; it 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'. As that indicates, there may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.
4.43 and 4.44	18. Are there any international standards for ethical policies or plans that you think entities must take into account when retaining and analysing biometric information for the purposes of fraud detection, prevention or investigation?	Suggest alignment with the Digital Forensics' Certification Board (DFCB)4 or NIST research5 or similar. Potentially combining ethical requirements for the management, storage and use of biometric information related to 1:1 matching with these forensic standards (ISO and NIST).

[4] Code of Ethics and Standards of Professional Conduct – Digital Forensics Certification Board (dfcb.org)
[5] NIST Publishes Review of Digital Forensic Methods | NIST

4.43 and 4.44	19. Do you have any suggestions or feedback regarding the Rules for the safe retention of biometric information for fraud or testing purposes?	No comment due to limited time to consider.

Chapter 4 - Privacy free text response

Rule number	Page/Section/Topic	Our Response
4.35 Compliance with the privacy governance code	Page 38, Part 3 - Privacy S4.35(1) and (2)	Noting as a non-APP entity we would need to voluntarily opt into the Code, or the Code may require amendment.
4.43 Requirements	Page 40, S4.43(1)	Data minimisation in compliance with S46(5)(d) of the Act – not more than 14 days after it was collected.

Chapter 4 - Usability and Accessibility

Rule/Section	Guide Question	Our response
4.46	20. Do you agree with the updated WCAG rule?	Yes, in principle.
4.46	21. If you answered no to the above question, please provide your reasoning.	N/A.

4.46	22. Do you have any feedback or suggestions regarding the updated WCAG rule?	No comment due to limited time to consider.

Chapter 4 - Usability and Accessibility free text response

Rule number	Page/Section/Topic	Our Response
		No comment.

Chapter 5 – Identity Service Provider

Rule/Section	Guide Question	Our response
5.2	23. Do you agree with the inclusion of the rule for accredited identity service providers requiring them not to generate a Digital ID for an individual under 14 years?	Yes – under 14 years is not in keeping with community expectations, or with certain services who do permit a young person of 14 to have an account that may interact with an Identity Service Provider or be required for a Relying Party.
5.2	24. Do you agree with the age of consent for the creation and use of a digital ID being changed to 14 years of age?	Yes – as noted this would be for consistency across several Commonwealth and Health services, there may also be some State/Territory services for which this is reasonable or required.
5.2	25. If you answered no to the above questions, please provide your reasoning	N/A.

Chapter 5, Part 2, Division 1	26. Do you agree with the inclusion of one-off digital IDs?	Yes, in principle.
Chapter 5, Part 2, Division 1	27. If you answered no to the above question, please provide your reasoning	N/A.
Chapter 5, Part 2, Division 1	28. Are there any risks or issues with the controls for the one-off digital ID service?	No comment.
Chapter 5, Part 2, Division 3, Subdivision 1	29. Are there any risks or issues with the proposed verification rules?	No comment.
Chapter 5, Part 2, Division 3, Subdivision 1	30. Do you have any proposals or suggestions for further clarifications for the verification rules?	No comment.
5.24, 5.30 and 5.31	31. Do you agree with the inclusion of eIDVT as a biometric matching method at IP2 plus only?	Yes, in principle.
5.24, 5.30 and 5.31	32. If you answered no to the above question, please provide your reasoning	N/A.

5.24, 5.30 and 5.31	33. Are there any risks or issues with the proposed inclusion of eIDVT as a biometric matching method at IP2 Plus only?	No comment.
5.24, 5.30 and 5.31	34. What are your thoughts on allowing eIDVT to meet the biometric binding requirements for IP3?	Reasonable, pending further confirmation for consistency between State/Territory providers.
5.24, 5.30 and 5.31	35. Are there any risks or issues with the proposed rules regarding the testing of eIDVT? Please refer to specific rules in your feedback where possible.	No comment.
5.24, 5.30 and 5.31	36. eIDVT has been restricted to Australian drivers licences and Australian passports. Do you think it should be expanded to other credentials in Schedule 1 Credential Requirements (such as proof of age cards)?	Yes, many individuals do not have a Passport or Drivers Licence.
5.24, 5.30 and 5.31	37. eIDVT could be used for the verification of foreign identity credentials in the future, do you think there is room to expand the digital ID identity proofing rules	No comment.

	to include the proofing of foreign credentials?	
5.31	38. Do you have any feedback or suggestions regarding the proposed document liveness rules?	No comment.

Chapter 5 – Identity Service Provider rules free text response

Rule number	Page/Section/Topic	Our Response
		No comment.

Chapter 5 – Attribute Service Providers

Rule/Section	Guide Question	Our response
Chapter 5, Part 3	39. Do you have any feedback or suggestions regarding the proposed rules for Attribute Service Providers?	No comment.

Chapter 5 – Attribute Service Provider rules free text response

Rule number	Page/Section/Topic	Our Response
		No comment.

Chapter 5 – Authentication Management Standard

Rule/Section	Guide Question	Our response
Chapter 5, Part 4, Division 4	40. Do you agree with the inclusion of in-device biometric capability as a method of unlocking authentication factors up to AL2?	Not sure. We would like to see this functionality geofenced to only be available when in Australia.
Chapter 5, Part 4, Division 4	41. If you answered no to the above question, please provide your reasoning	N/A.
Chapter 5, Part 4, Division 4	42. Do you have any feedback or suggestions regarding the proposed rules for the inclusion of in-device biometric capability for authentication?	See comment above.

Chapter 5 – Authentication Management Standard free text response

Rule number	Page/Section/Topic	Our Response
		No comment.

Chapter 5 – Identity Exchanges

Rule/Section	Guide Question	Our response
Chapter 5, Part 5	43. Do you have any feedback or suggestions regarding the proposed rules for identity exchanges?	No comment.

Chapter 5 – Identity Exchanges free text response

Rule number	Page/Section/Topic	Our Response
5.84 – Annual Transparency Report	Page 96, S5.84(3)	Agree that no personal information of the individual should be published, however, there should be some scrutiny over this, in regard to the possibility for requests linked on dates to major events of significance where the individuals subject to a request may become re-identifiable on the basis of other publicly available information is something that should be given some consideration and oversight. The type of enforcement body, or the date may be sufficient to identify incidents of importance, or that are covered by the open media.
5.84 – Annual Transparency Report	Page 96, S5.84(3)	Suggest the inclusion of a clause to reflect the above issue where the Regulator may on review decide not to publish certain incidents as recorded.
5.84 – Annual Transparency Report	Page 96, S5.84(3)	See noted in the Guide Questions on the Digital ID Bill and Digital ID Rule at Q/21 on Privacy protections – notes on Enforcement bodies.

Chapter 6

Rule/Section	Guide Question	Our response
6.1 and 6.2	44. Are there any risks or issues with the proposed rules for material changes assessment during the annual review?	No comment due to limited time to consider.
6.1 and 6.2	45. Do you have any feedback or suggestions regarding the proposed rules for annual assessments?	No comment due to limited time to consider.
6.3 and 6.4	46. Do you agree with the policy requiring the protective security and fraud assurance assessments to be conducted at a 2 year cycle?	This is reasonable.
6.3 and 6.4	47. Please provide any detailed feedback or suggestions regarding the change to a 2 year assessment cycle.	Supported due to the continual emerging new risks and technology advancement in the digital world.

Chapter 6 – free text response

Rule number	Page/Section/Topic	Our Response
		No comment.

Additional feedback – Nil.