07 October 2023

Department of Finance

SUBMISSION: DIGITAL ID BILL 2023 EXPOSURE DRAFT

IIS Partners

INFORMATION INTEGRITY SOLUTIONS

Contents

7 October 2023

John Shepherd
First Assistant Secretary, Digital ID Taskforce
Department of Finance
1 Canberra Avenue
Forrest ACT 2603
[Submitted electronically]

Dear Mr Shepherd

IIS Partners submission to the Digital ID Bill 2023 Exposure Draft

Overall, IIS Partners (IIS) welcomes the changes seen in the Exposure Draft of the Digital ID Bill 2023 (the Bill) since a draft Bill along similar lines was issued in 2021. We find the range of privacy protections set out in Chapter 3 of the Bill to address areas of risk to be particularly important and welcome.

Nevertheless, further improvement is needed from an individual user standpoint before digital ID systems including the Australian Government Digital Identity System (AGDIS) could be considered trustworthy and safe for an individual to use. The system is strong but not strong enough. The community must have total trust and confidence in the system. Anything less would defeat the central objective of a very inclusive, widespread take-up of digital IDs and all the benefits that accrue from having secure and reliable online identity verification and authentication.

The Minister of Finance and the Department of Finance have stated that the new Digital ID System should be **"Secure, Convenient, Voluntary, and Inclusive".** Many of the concerns we raised in previous consultations and engagements still stand and still require attention, especially in light to these stated goals. Of those points we are most concerned by:

- The Bill's overly permissive approach to law enforcement access to information handled and generated by digital ID systems, provided for under broad exceptions permitting disclosure. This approach will negatively impact trust in the system which in turn will **negatively impact Inclusion** especially those individuals marginally attached to society.
- Exceptions to voluntary use contained in the Bill which would allow encroachment on the intended 'voluntariness' of AGDIS over time **negatively impacts Voluntary**, especially in the hands of an overzealous future government.
- The risk that the interests of individuals will be overtaken by a focus on the needs and convenience of accredited entities and relying parties will **negatively impact Convenience**. The Bill can do more to ensure the interests of individuals are given greater influence in advisory committees and future legislative review.

IIS Partners
INFORMATION INTEGRITY SOLUTIONS

- The risk that inadequate funding of key regulators results in ineffective oversight arrangements will **negatively impact all the goals of Secure, Convenient, Voluntary, and Inclusive and lower Trust**. Appropriate dedicated funding must be allocated to the Australian Competition and Consumer Commission, acting as the Digital ID Regulator, and the Office of the Australian Information Commissioner (OAIC), overseeing and enforcing the privacy aspects of the scheme.

Put simply, the public not only expects protection *by* government and its regulators in the operation of the new system, it expects similarly strong protection *from* government particularly in a system that is potentially so central to everyday life. Failure to address concerns such as these and the ensuing lack of trust were some of the most significant reasons why the Australia Card initiative failed in 1988 and the Access Card initiative failed in 2007.

We would be pleased to discuss any aspect of our submission and thank the Department for the opportunity to provide these perspectives. If you have any questions or need additional information, please do not hesitate to contact us. Our more detailed comments on the Bill follow.

Kind regards

[redacted]

Malcolm Crompton AM, CIPP
Founder and Partner

[redacted]

Nicole Stephensen
Partner

[redacted]

Michael S. Trovato, CISA, CISM, CDSPE
Managing Partner

Information Integrity Solutions Pty Ltd
PO Box 978, Strawberry Hills NSW 2012, Australia

Contact at iispartners.com

1. Feedback on accreditation provisions in the Bill

1.1 Accreditation and conditions imposed by the Regulator

Page 16 of the Guide to the Bill asks stakeholders whether the Regulator's power to impose conditions on accreditation is 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?

We believe the Bill gets the balance right here. Our understanding is that the Regulator may impose special conditions on accreditation that allow an entity to collect biometric information or restricted attributes (such as passport numbers or health information). It is better that the Bill creates a high bar of protection which the Regulator can adjust for certain specific entities.

The alternative – that the Bill creates a lower bar of protection in the name of consistency among accredited entities – would be a poor outcome. The current approach imposes the principle of data minimisation – that certain data is restricted – with a strong framework of oversight in the form of Regulator approval for any expansions in collection activities.

We believe the Bill gets the balance right in relation to the Regulator's power to impose conditions on accreditation. We would not support a change that weakened this approach or allowed wider collection and handling of biometric information or restricted attributes without Regulator approval.

2. Feedback on privacy provisions in the Bill

Our feedback in this section is focused on strengthening privacy arrangements and reducing risks of creeping surveillance or weakening of provisions by overly permissive exceptions. The comments below largely relate to Chapter 3 in the Bill.

2.1 Coverage of the Privacy Act and APP-equivalent agreements

IIS supports the privacy provisions contained in Chapter 3, Part 1 and Part 2, Division 1 – specifically, that accredited entities are bound by the Australian Privacy Principles (APPs) contained in the Privacy Act or an equivalent state or territory privacy law. This ensures appropriate extension of existing regulatory frameworks rather than duplication of privacy requirements.

Clauses 35 and 36 are particularly important in ensuring that a breach of an APP-equivalent agreement or the additional privacy safeguards contained in Division 2 is brought under the jurisdiction of that Act and subject to that Act's regulatory and enforcement provisions. This will mean that privacy non-compliance in relation to the digital ID scheme will receive the same regulatory protection as privacy non-compliance generally.

We also support the extension of the definition of personal information to include attributes of individuals (where those attributes are not otherwise covered by the definition) as provided for under clause 33.

We support the privacy provisions contained in Chapter 3, Part 1 and Part 2 Division 1 and do not support any weakening of those provisions.

2.2 Restrictions on disclosure of unique identifiers

Enhanced or excessive surveillance of individuals transacting online is a major privacy risk point for any digital ID system. Unique identifiers heighten surveillance and tracking risks by allowing an individual's disparate activities and transactions online to be linked and for detailed information about the individual to be accrued over time. They also facilitate, and exacerbate the impact of, identity theft.

IIS therefore supports the restrictions provided for under clause 44, except for the broad permissions for law enforcement purposes, as established by clause 44(4)(e).

While certain exceptions may be necessary for managing the integrity of digital ID systems, IIS is against broad permissions for law enforcement purposes, as established by clause 44(4)(e). Trading away individual freedoms and anonymity for small gains in investigative convenience, especially where an investigation is unrelated to the integrity of the digital ID system itself, is a poor outcome for individuals and risks fostering mistrust in digital ID systems.

We recommend removal of the exception allowing disclosure of a unique identifier for the purpose of 'detecting, reporting, investigating or prosecuting an offence against a law of the Commonwealth, a State

or a Territory.' If this exception is retained, it should be amended to apply to very serious criminal offences only, such as terrorism, murder, child abuse, or large-scale organised crime (for example, where the crime is suspected to involve more than $10 million). Accredited entities should not be compelled to disclose unique identifiers for minor offences. (Law enforcement exceptions are discussed in greater detail in Section 3 of this submission.)

We recommend removing clause 44(4)(e). If clause 44(4)(e) is retained, narrowing it to apply to very serious criminal offences only.

2.3 Protections for biometric information

Biometric information carries many of the same risks as unique identifiers generally with the added danger of being difficult to recoup or 'reissue' if compromised. Certainly, its capacity to intensify surveillance of individuals is well understood.

We are therefore in favour of strict protections for the collection and handling of biometric information in conjunction with digital ID systems. To that end, we support the prohibition of use of biometric information for one-to-many matching provided for under clause 45(2). We also support strong and specific deletion requirements, including those contained in clause 48 and associated deletion requirements in the Accreditation Rules. Deletion arrangements should be strict and as short as is practicable.

Clause 48(2) requires an accredited entity to destroy biometric information immediately if an individual withdraws their consent. We commend the formalisation of consent withdrawal in the legislation as this offers individuals greater control over their biometric information. However, this provision would provide stronger protection if it also required accredited entities to make consent withdrawal easy and straightforward for individuals.

Strengthening consent withdrawal along these lines would accord with the recent review of the Privacy Act which proposed that that Act be amended not only to expressly recognise the ability to withdraw consent, but also for withdrawal to occur 'in a manner as easily as the provision of consent' – a proposal to which the Government has 'agreed in principle.'[1] As is, the consent withdrawal provision in the Bill risks ineffectiveness, particularly if people are discouraged from pursuing it either because they are unaware of their right to withdraw consent or because the process is needlessly complex.

We support the prohibition on one-to-many matching and strict deletion arrangements in relation to biometric information and would not support any weakening of those provisions.

We also support the consent withdrawal right contained in clause 48(2) but recommend it be strengthened to require that withdrawal of consent be as prominent and easy as providing consent.

[1] See *Government Response: Privacy Act Review Report*, Proposal 11.3, p 26.

2.4 Disclosure of biometric information to law enforcement

Clause 46(3) permits disclosure of biometric information to a law enforcement agency either under a warrant issued by a magistrate, judge, or member of a tribunal *or* with the consent of the individual. This is a higher bar than other law enforcement exceptions contained in the Bill and reflects the sensitivity of biometric information. However, our view remains that disclosure of *any* digital ID information to law enforcement significantly weakens the trust individuals will have in digital ID systems in Australia.

There is a strong public interest in having trusted digital ID arrangements in Australia and preventing incremental expansion in the surveillance activities of law enforcement agencies over use of the digital ID system. The public interest in an inclusive, widely used, trusted digital ID system significantly outweighs the public interest in the marginal improvement in law enforcement that might arise from removing barriers for law enforcement activities. (Law enforcement exceptions are discussed in greater detail in Section 3.)

We recommend that clause 46(3) be removed. If it is retained, narrow it to allow disclosure only in relation to very serious criminal offences such as terrorism, murder, child abuse, or large-scale organised crime (for example, where the crime is suspected to involve more than $10 million). It should also continue to be subject to the warrant requirement contained in clause 46(3)(a).

2.5 Prohibition on data profiling and online tracking

A central concern for digital ID systems is preventing the development of an extensive data profiling and tracking apparatus built from the foundation created by legitimate online verification and authentication activities. We therefore support provisions to mitigate this risk – particularly clause 50. That said, clause 50 would be stronger if it did not limit its ambit to 'personal information'.

It has been well established in recent years that a major difficulty in securing privacy in the digital age is that much online tracking activity falls outside the definition of 'personal information' and therefore outside the operation of privacy laws. This issue was given particular attention in the recent review of the Privacy Act with the review recommending both that the definition of personal information be broadened to capture online identifiers and that the Privacy Act regulate online targeting, including where it involves use of deidentified and unidentified information.[2]

In our view, clause 50 would be stronger and more effective at curbing online tracking if clause 50(1)(a) were removed. The remaining parameters set out in clause 50(1)(b) are specific enough to achieve the objectives of this provision.

We strongly support clause 50(2) which provides important protection against accredited entity overreach and/or coercion of individuals using their services. We would not support weakening or removing this provision.

---

2 See *Government Response: Privacy Act Review Report*, series 20 proposals, p 32.

2.6 Restrictions on data retention by identity exchanges

Clause 53 prohibits identity exchanges from retaining certain prescribed attributes of individuals. This provision is essential to ensuring that identity exchanges do not, over time, accrue detailed information about individuals and their activities online.

We support clause 53 and would not support any change that weakens its operation in practice.

3. Feedback on law enforcement exceptions in the Bill

IIS has been on the record in previous submissions regarding our concern about law enforcement exceptions which we find to be too broad, establishing too low a bar for disclosure to law enforcement agencies and too weak a framework for oversight. There are several law enforcement exceptions contained in the Bill including clause 44(4)(e) discussed above in Section 2.2, clause 46(3) discussed above in Section 2.4 and clause 51.

Guaranteeing in law that national security, law enforcement agencies and other enforcement bodies are excluded from access to information in the digital ID system may be the most crucial remaining step in ensuring that the system is trusted and so genuinely inclusive.

Vulnerable groups often have the lowest trust in government and its agencies. They are often also the people who have most interaction with government. Everything must be done to ensure the system can be trusted from their perspective or the goal of inclusion could be severely compromised.

3.1 Risks of law enforcement exceptions

The guide accompanying the Bill states that the clause 51 offers tighter law enforcement provisions than equivalent provisions contained in the Privacy Act, but this is misleading. The Privacy Act is a generalist law. Laws that regulate specific systems – such as those governing the Census,[3] *My Health Records*,[4] healthcare identifiers[5] and COVID-19 contact tracing[6] – contain much tighter restrictions on law enforcement access.

In the case of the Census and COVID-19 contact tracing, no law enforcement access is permitted at all. These laws are a more relevant point of comparison because, like the Digital ID Bill, they deal with potentially highly privacy invasive scenarios – scenarios in which, for example, the information handled may be particularly sensitive or where information may have to be shared between multiple parties or where unique identifiers may be used or where there are risks of tracking or intrusion in the private affairs of ordinary citizens.

In each of the cases above, there was also a recognition at the time the laws were being developed that trust in the system was a first priority and that the trust might be quickly eroded by overly permissive law enforcement exceptions. In such cases, the public interest in supporting effective statistics collection, healthcare delivery, or pandemic response, outweighed the public interest in any potential facilitation of law enforcement activities.

---

3 See *Census and Statistics Act 1905 (Cth).*

4 See *My Health Records Act 2012 (Cth).*

5 See *Healthcare Identifiers Act 2010 (Cth).*

6 See *Privacy Amendment (Public Health Contact Information) Act 2020 (Cth).*

Digital ID systems – particularly AGDIS – are in the same category. The public interest in establishing strong, trustworthy digital, widely used, inclusive ID systems – systems that allow safe access to online services, systems that protect individuals from needless online tracking or identity theft – outweighs the public interest in any potential facilitation of law enforcement activities. Without strict prohibitions, digital ID systems risk becoming de facto surveillance tools for law enforcement.

We therefore strongly recommend the removal of clauses 44(4)(e), 46(3), 51 and any others which permit information handling for law enforcement purposes.

If, against advice, those provisions are retained, narrow them to allow information handling or disclosure only in relation to very serious criminal offences such as terrorism, murder, child abuse, or large-scale organised crime (for example, where the crime is suspected to involve more than $10 million). They should also be subject to a requirement that information access be conditional on the issuing of a warrant or order by a magistrate's court or higher court.

3.2 Uncertainty about the effect of other law enforcement or national security legislation

Restrictions applying to law enforcement access will be moot if other legislation continues to authorise access to information and override protections contained in the Bill. Currently the Bill is silent on the powers that enforcement and national security agencies have been given, particularly in other recently introduced legislation such as the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*; the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2020*; and possibly the *Security Legislation Amendment (Critical Infrastructure) Act 2021*.

Without provisions similar to Section 94ZD of the *Privacy Amendment (Public Health Contact Information) Act 2020* to ensure that the Digital ID Bill prevails over the powers and processes contained in these and other laws, there is a risk of unwarranted, broadscale national security and law enforcement intrusion in the digital ID systems provided for under the Bill.

We strongly recommend addressing this gap in protection and ensuring the Digital ID Bill prevails over other laws authorising information access and disclosure for law enforcement purposes.

4. Feedback on 'voluntariness' and community protections

4.1 Voluntariness

Guaranteeing that participation in digital ID systems will be voluntary and non-compulsory is one of the strongest protections available to individuals to avoid overreach by government or other entities and worsening of the power imbalance over individuals. Ensuring non-compulsory participation is particularly important for AGDIS. As the guide to the Bill points out, 'unlike a typical market for services, Australians do not have a choice to go to another provider if they want to obtain government assistance.'[7] The guide goes on to say that 'for Australians who are unwilling or unable to access taxpayer funded services online, the Bill will ensure that using a Digital ID to access government services through the AGDIS is voluntary.'[8]

This guarantee must also be permanent and unequivocal. Previous governments have failed to live by commitments to voluntary or 'opt in' arrangements especially when establishing new digital services. At times, the speed with which such commitments have been traduced to 'opt out' or no choice at all has been embarrassing. The change from 'opt in' with the Personally Controlled Electronic Health Record to an 'opt out' or no choice at all My Health Record is a recent example.

We therefore commend the Minister on the clear and repeated commitments she has already made that the use of a digital identity will be voluntary and recommend the Minister and her counterpart in the House repeat the commitment in the strongest terms when introducing the legislation to Parliament.

4.2 Exceptions to voluntariness

Clause 71(3) establishes exceptions to the requirement that digital IDs used in conjunction with AGDIS be voluntary. The guide to the Bill (p 26) asks stakeholders whether the balance between voluntary use and the exceptions to voluntary use is right and whether any additional exceptions are appropriate.

We do not support the creation of additional exceptions and is concerned about the nature and scope of those set out in clause 71(3) which seriously impinge on the stated intention of voluntariness. We are particularly concerned with clause 71(3)(a) which would override the voluntary use requirement where 'a law of the Commonwealth, a State or a Territory requires verification of the individual's identity solely by means of a digital ID.' IIS understands, from discussions with representatives from the Department of Finance, that there is currently no plan or intention to introduce any legislation to trigger this exception or amend existing legislation, at the Commonwealth level at least.

---

7 Department of Finance, Your guide to the Digital ID legislation and Digital ID Rules, 18 Sept 2023, p 26.

8 Department of Finance, Your guide to the Digital ID legislation and Digital ID Rules, 18 Sept 2023, p 26.

This means that clause 71(3)(a) exists only as a convenient 'override button' to voluntary use, allowing future encroachment on voluntary use by stealth. There is a clear risk that, over time, as the AGDIS is taken up by individuals, the Government finds increasing justification for reasons of cost and efficiency to make digital IDs a primary channel for access to government services. As it stands, the Bill would create no protection against this.

Existing and new legislation need only trigger clause 71(3)(a) to make digital IDs compulsory for certain government services. Given that it is citizens of lower socio-economic standing that are more likely to rely on government services and benefits, it will be those citizens that will be most affected by encroachments on voluntary use. This would appear to contradict not only the Minister's commitment to voluntariness but also her commitment to inclusivity – that no marginalised demographic group will receive differential treatment or lesser choice and control than any other group.

We recommend that s71(3)(a) and (b) be removed. If that is not possible, those subsections should be subject to appropriate oversight, for example approval by the Digital ID Regulator or the OAIC.

4.3 Ensuring community voices are heard and acted on

It is easy to forget that one of the most important beneficiaries of the proposed system are everyday individuals and not just relying parties. Indeed, it is their lives that could be most adversely affected by a poorly operated, needlessly intrusive digital ID system. In the extreme, individuals could be asked to trade away their civil liberties and privacy to access basic services. Past efforts to introduce comprehensive identity systems – including the Australia Card and the Access Card – have failed due to the privacy concerns and distrust of ordinary Australians. The impact of loss of community trust should therefore not be underestimated.

Clause 91 empowers the Minister to establish advisory committees, however this clause gives the Minister discretion as to their composition and terms of reference. There is no requirement for membership to include a person representing the interests of civil society.

Given the potential for a digital ID system to seriously impact the interests and privacy of the individual, we recommend that stronger advisory processes be established that ensure the perspective of individual users is given more influence. Options for more influential involvement include establishment of a board on which the interests of civil society are represented and which has decision-making powers over crucial matters such as definitional issues (for example, the definition of identity or additional categories of information that should be classed as restricted or prohibited) and changes to the Digital ID Rules and Accreditation Rules. The board should also have the power to report directly to Parliament. Establishing a board of this kind would be a meaningful and practical way for the Minister to demonstrate her stated commitment to digital ID systems that are 'secure, convenient, voluntary, and inclusive.'

We therefore recommend that clause 91 be expanded to require the creation of a user experience, privacy, and security board rather than leave its creation to the discretion of the Minister and that the composition of the board be spelt out in the Bill. Specifically, the Bill should require that the interests of civil society be given dominant representation.

4.4 Ensuring community voices are heard in any advisory committee

We suggest that clause 91 be amended to give assurance of community representation on any advisory committee.

If our recommendation for a user experience, privacy, and security board is not taken up, we suggest clause 91 provide for at least one advisory committee whose main focus is on addressing areas of potential concern from an individual or user perspective.

We also recommend that clause 91 require membership on all advisory committees of at least one individual representing the interests of civil society.

4.5 Ensuring community voices are heard during review of the Act

Clause 153 requires a review of the operation of the Act to be conducted within two years of the commencement of the Act. While any such review is likely to involve some form of open stakeholder consultation, our concern is that the views of civil society will not be heard, particularly given the subject-matter expertise required to engagement meaningfully and the financial constraints that commonly restrict the advocacy activities of civil society groups.

In line with our comments above about the importance of community input, we recommend that clause 153 be amended to require that the review of the legislation be supported by an advisory committee at least a third of whose membership comprises individuals representing the interests of civil society.

5. Feedback on resilience

5.1 Cyber security incidents

In Section 9 ‘Definitions’ there are some specific and prescriptive definitions that the Bill drafters probably intended to be comprehensive and give the Digital ID Regulator criteria for various actions and remedies to ensure trust in the system, and in particular at page 6 line 21, from a security perspective.

We support the strong provisions for cyber security, as a key reason to implement a trusted Digital ID System is to help combat cyber-crime.

However, the cyber security incident definitions only focus on unauthorised access or impairment vs unintentional conditions.

With that in mind, we recommend that Bill be revised to consider the Australian Signals Directorate’s Australian Cyber Security Centre website’s ‘Guidelines for Cyber Security Incidents’ definition of a cyber security incident, “*A cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that has either compromised business operations or has a significant probability of compromising business operations.”*

In the text of the Bill, there are 10 other instances of the term ‘cyber security incident’. The Bill references the definition with respect to suspension of accreditation; revocation of accreditation; restricting the disclosure of a unique identifier; compliance assessments; and suspension of approval to participate in the Australian Government Digital ID System.

A broader definition would empower the Digital ID regulator to set a high bar for resilience of the Digital ID System and thereby help ensure security and trust.

We recommend broadening the definition of cyber security incident to include accidental or inadvertent (for example, due to poor risk management or operational controls).

6. Feedback on regulatory arrangements

6.1 Appropriate funding to ensure strong enforcement and oversight

We remain concerned about the funding available to the regulators to provide credible oversight, enforcement and remediation to individuals affected by inappropriate action or inaction by any accredited entity or relying party in the system.

The funding for the OAIC to undertake its current obligations has been so manifestly inadequate for decades that it has not been an effective regulator for a long time. If the government expects to create trust in the privacy protections applying to accredited entities and relying parties, it must provide the OAIC with a very significant step-up in funding, possibly a doubling of current funding. Similarly, the government must provide adequate additional funding to the Digital ID Regulator for the same reason.

Too often, new legislation is introduced without commensurate funding for its implementation or enforcement. Instead, the funding is left to be settled in subsequent federal Budgets. Budget exigencies are then offered as the reason for not providing sufficient funding.

We are so concerned about trust in the effective oversight and enforcement of the legislation that IIS recommends the legislation should only be introduced to Parliament if it is accompanied by legislation to appropriate the funds to the relevant regulators that would enable them to enforce credibly and remediate harms that individuals using the system might suffer.

In summary, we recommend the Digital ID Bill be accompanied by legislation to appropriate funds to the Digital ID Regulator and the OAIC. If that is not possible, the Digital ID Bill should be accompanied a statement to Parliament by the Minister for Finance that commits the Government to providing specified additional funding.

6.2 Rapid resolution of complaints

Separate from funding issues, one of the key issues with the OAIC is that its process do not facilitate rapid resolution of complaints or investigations. Procedural fairness requirements make it a long and drawn-out affair regardless of funding. This alone justifies the obligation in the law that use of a digital identity must remain at all times voluntary so that individuals have a fall-back alternative.

Preferably, we recommend including in the Bill a new pathway for rapid resolution of problems associated with creating and using digital identities. We also suggest that the legislation include procedures that enable the Digital ID Regulator and the OAIC to provide fast initial redress pending final decisions.

INFORMATION INTEGRITY SOLUTIONS PTY LTD
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
E: contact@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN 107 611 898

IIS Partners
INFORMATION INTEGRITY SOLUTIONS