aiia
australian information
industry association

Review of National Arrangements for the Protection and Management of Identity Information

Date: 26 October 2018

Level 1, 131 Canberra Ave
Griffith ACT 2603
Australia

61 2 6281 9400
info@aiia.com.au
www.aiia.com.au

About AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. AIIA is a not-for-profit organisation that has, since 1978, pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment and drive Australia's social and economic prosperity.

AIIA does this by providing a strong voice on policy priorities; creating a sense of community through events and education; enabling a dynamic network of collaboration and inspiration; and curating compelling content and relevant information.

AIIA's members range from start-ups and the incubators that house them, to small and medium-sized businesses including many 'scale-ups' and large Australian and global organisations. We represent global brands including Apple, Adobe, Cisco, Deloitte, DXC, Gartner, Google, IBM, Infosys, KPMG, Lenovo, Microsoft and Oracle; international companies including Optus and Telstra; national companies including Ajilon, Data#3, Technology One, SMEs including Technovate and Silverstone Edge and start-ups such as OKRDY. While AIIA's members represent around two-thirds of the technology revenues in Australia, more than 90% of our members are SMEs.

Our national board represents the diversity of the digital economy. More detailed information about the AIIA is available on our web site: www.aiia.com.au

AIIA appreciates the opportunity to provide input to the review and gives consent for this submission to be published.

1.1 Issues for consideration

This section identifies a range of issues identified by AIIA members in the expectation that, while not discussed in the consultative process, will be addressed in the Review Report.

The AIIA considers the scope of the review to be extremely ambitious, particularly in the timeframe that has been allowed for consultation and comment. The Association considers there to be a significant risk that key stakeholders will not be afforded adequate time to make representations to the Department on this important issue.

The AIIA also notes that user expectations and needs with respect to identity and identity management are critically important particularly from a privacy perspective and should be accorded a high priority by the Department when framing its recommendations.

As services move from face to face to online there has been a subtle shift from possession and presentation of the credential itself to presentation and verification of the information it contains. The Document Verification Service (DVS[1]) provides a mechanism whereby agencies and businesses can verify with the issuing agency information contained on or in a given credential.

AIIA would argue that, in the context of improved service delivery, privacy and the user experience, the real issue confronting individuals (and businesses) is having to prove who they are online multiple times and having to manage multiple authentication credentials issued by agencies providing services.

The AIIA considers that agencies should rely on commercial services (as opposed to investing heavily in in-house verification and credentialing systems) for the delivery and maintenance of identity management services as this represents a more efficient use of government resources and enables agencies to focus on their core business - service provision to individuals and businesses.

AIIA is also concerned that there are too many documents/credentials that are able to be used by an individual in an identity verification. The NIPGs reference a wide range of possible documents,

[1] See https://www.dvs.gov.au/Pages/default.aspx

particularly in the Secondary Use in the Community category and the NIPGs make it an agency's responsibility to determine both document weightings and types on which it will rely. While this goes to the heart of inclusiveness and accessibility by enabling people from diverse environments and personal situations to have the best opportunity possible to establish their identity with a government agency, it does necessarily increase the scope for identity fraud.

In terms of establishing an individual's "social footprint" has consideration been given to seeking consent from the individual to establish their presence in different social media? If so has a privacy assessment been undertaken.

If there are no national capabilities to identify fraudulent identities is there value in retaining it as a necessary component of the NIPGs (and by inference the TDIF). What is also unclear is whether it is the Department's intention to establish such a capability. If so how would such a database be established and maintained? Are there particular human rights and privacy issues associated with maintaining such a database?

The review also raises questions about the department's view on the use of biometrics generally and in what circumstances would it sanction (i) retention and (ii) sharing of biometrics by an agency with (a) another agency and (b) a private sector organisation? It is assumed that any and all identity information including biometric data would be stored by an agency / identity provider in an encrypted form. Under what circumstances would an interception agency be entitled to require the agency or identity provider to make that data available to the agency?

The AIIA would note that much of the data regarding the magnitude of "identity crime" is based on the report *Identity Crime and Misuse in Australia 2016*. The AIIA notes that excluding certain types of financial crime will significantly reduce the overall financial impact of what is defined as identity crime. While it may be considered a definitional issue, overstating the impact of identity crime has in the past been used as a basis for the introduction of new identity security initiatives that impose undue burdens on civil society.

In considering the magnitude of identity crime and this current review has the Department:

- Established a up to date evidence base to justify the review or is it the intention of this review to create / obtain the evidence required to underpin intended policy initiatives?

  At the consultation session it was stated that the review team already knew what recommendations it was going to make. This is of concern to AIIA members, that is, the conclusions have already been drawn prior to the completion of the consultation process.

- Undertaken risk assessment of different compromise scenarios in terms of their likelihood and consequence? It would be useful to understand to what extent do these results demonstrate an imperative to strengthen registration/enrolment processes and to increase the extent to which identity data is shared across agencies.

The AIIA considers that before moving fully into the digital identity space the broad community needs to have confidence that identity information is being appropriately secured. The evidence in the form of data breaches from both government and commercial entities suggest that identity security requires strengthening. Accountability, auditing, compliance testing and public reporting need to be introduced in order to demonstrate that personal information is being adequately protected. Simple steps such as securing government websites are a good beginning.

Any investigation or review of identity credentials and identity assurance must involve a privacy impact assessment. The Trusted Digital Identity Framework (TDIF) developed by the Digital Transformation Agency has and will continue to undergo independent privacy assessments. Therefore, the AIIA considers that recommendations to change the processes by which "identity credentials" are issued (e.g. such as biometrically anchoring all credentials) must also be subject to independent privacy assessments.

1.2 Key recommendations

AIIA have three key recommendations.

1. Clarify objectives of the review – it is unclear what arrangements the review seeks to enhance or strengthen - and whether all or some government and private sector issuance and management of identity information is in scope;

    a. As a subset of this, there needs to be clarity about how this review relates to other initiatives that the Commonwealth is engaged in around the use and management of identity information, particularly the Facial Verification System and the Digital Transformation Agency's Digital Identity Framework;

2. If the review is truly concerned about the effect of identity crimes on Australians, then a copy of the the draft review report should be made available for public comment; and

3. Consider the adoption of federated model especially with existing identity service providers at Federal and State/Territory levels of government with agreed interoperability protocols and standards as we transition to digital ID. The federated model should apply to commercial identity issuers especially the financial sector as well as government issuers.

These recommendations are discussed in more detail below.

1.3 Detailed Discussion

Objectives unclear

The AIIA is keen to understand how this review will impact on government and industry work on the development of Digital ID solutions. The relationship between this review and Digital ID activities being undertaken by governments at both the federal and state level (e.g. DTA and ServiceNSW etc.) is unclear as are its implications for the commercial identity verification activities of businesses such as GreenID and Vix Verify. The time trajectory for this review and the activities of other agencies appears out of synch suggesting a lack of coordination and communication, particularly at the Federal level of government.

At the industry consultation the issue of biometrics was raised in the context of strengthening existing identity credentials but there was little substantive discussion beyond a suggestion that biometrics would be part of the review's recommendations. Any recommendation for the expansion of biometric capture and their use in identity verification must be the subject of an independent privacy assessment and must not involve the creation of a centralised biometric database. Consideration should also be given to constraining the type of biometrics that are able to be collected by agencies for the purpose of identifying individuals.

From the terms of reference and following the industry consultation process it remains unclear

1. which arrangements/legislative or practices and systems for the collection, use, sharing of identity information or coordination activities between government agencies and other entities are currently under consideration under this review.

2. whether the identity crimes referred to are the result of poor handling of identity information being held by government agencies under current arrangements and practices and systems, or the loss / compromise of documents used by citizens for identity-proofing;

3. what is the evidence to support the increase in identity crimes in the public sector vs private sector? Data has not been made available to support this claim. Review investigation and findings should be supported by data and a distinction should be drawn between diverse types of fraud e.g. identity fraud vs financial fraud (in particular card-not-present fraud);

4. whether this review will assess the relevance and appropriateness of the National Identity Security Strategy 2007 and the National Identity Proofing Guidelines 2014 in the context of the development by the DTA of the trusted Digital Identity Framework and the suite of international identity management and authentication standards;
5. how this review will impact if at all on the MyGov ID initiative of the ATO or the ID Exchange initiative of DHS; and
6. the level of compliance by agencies and integration with private sector organisations within existing arrangements and planned developments is unclear;

Draft review report should be made public

1. While consultation has been undertaken in different states and opportunities provided to make written submission, it is unclear whether the draft review report will be made available for public comment.
2. Therefore, clarity should be provided around what will happen to the draft review report. If this review is seeking to protect Australians from the threat of identity crime, then the draft review report should be made public for comments before its finalised.

Federated model should be adopted coupled with agreed interoperability protocols and standards

Moving forward we recommend,

1. the adoption of a Federated approach with the states, based on agreed interoperability protocols and standards for both issuance of identity documents/digital ID and storing of personal information;
2. planning for integration with commercial services, so Australians can nominate their preferred source for authentication, this should prepare for risk-based authentication and a trust-broker approach using tokens that allow citizens to control release of non-identity attributes e.g. over-18 as opposed to date-of-birth;
3. registration processes for identity verification should be standardised across jurisdictions based on agreed level of risks; and
4. mechanisms to minimise attribute transmission should be adopted e.g. facial images should not be sent to a central repository to support the facial verification service, visage templates[2] should be used.

AIIA members would be happy to meet with the Department to discuss these issues in more detail.

Kishwar Rahman
GM Policy and Advocacy

Australian Information Industry Association

Office 4, 131 Canberra Avenue, Griffith ACT 2603
M: 0498 807 238 P: 02 6281 9402 | k.rahman@aiia.com.au | www.aiia.com.au

[2] A visage template or face template is the mathematical representation of the key characteristics of an individual face that allow it to be distinguished from another – such as the distance between the eyes, the width of a mouth and other measurements – essentially the data about a face rather than the image.