Report to the Council of Australian Governments

A Review of the National Identity Security Strategy

2012

Table of contents

INTRODUCTION

Preserving and protecting a person's identity is a key concern and a right of all Australians. As such, the National Identity Security Strategy (NISS) aims to develop the conditions so:

Australians may confidently enjoy the benefits of a secure and protected identity.

Maintaining effective identity security across Australia is a shared responsibility – the Commonwealth, State and Territory governments have a significant role to play in this. It is a mutually beneficial role, as state-issued proof of identity credentials can be used to obtain Commonwealth proof of identity credentials, and vice versa. This means that any weak link within government agencies affects the wider identity security framework.

It was at a special meeting on Counter-Terrorism on 27 September 2005, that the Council of Australian Governments (COAG) agreed to develop and implement a national identity security strategy by way of an Intergovernmental Agreement (IGA). In 2007, the NISS IGA was signed by COAG leaders.

The NISS was developed with a focus on how identity security contributes to national security. It contained six key elements of work to enhance identity security in Australia:

1. registration and enrolment standards for use by agencies that enrol individuals to issue government documents that may also function as key documents for proof of identity
2. security standards for such documents to reduce the possibility of forgery or unauthorised alteration
3. improved ability for government agencies across jurisdictions to verify information on such documents
4. standards in the processing and recording of identity data to improve the accuracy of existing records (where appropriate) and to prevent the creation of inaccurate identity records in future
5. standards for government agencies to apply where they provide services to a person whose identity needs to be verified, and there are significant risks associated with the wrong person getting access to a service, and
6. measures to enhance the national interoperability (i.e. the ability of different computer systems to share data and work together) of biometric identity security measures.

This document reports on the triennial review of the NISS. Included is an evaluation of the achievements of jurisdictions, and a discussion of lessons learned. To continue the good work of the NISS and respond to the evolving identity environment in Australia, the review also includes a summary of action items.

The review was led by the National Identity Security Coordination Group (NISCG). The NISCG is chaired by the Commonwealth Attorney-General's Department and comprises representatives from: Commonwealth, State and Territory governments, the Council of Australasian Registrars, CertValid, Austroads, and the Office of the Australian Information Commissioner (Privacy).

EVALUATING THE NISS

An evaluation of each element of the NISS is below. Provided is a rationale for continued inclusion in the NISS, key achievements, and further work required.

REGISTRATION AND ENROLMENT STANDARDS

Rationale

Australians use a combination of credentials issued by different jurisdictions, as proof of identity. Consistent standards around enrolment and registration will improve confidence in the integrity of identity credentials, and reduce the risk of exploitation. This will also encourage digital service delivery, where identity is verified by reference to identity credentials.

There is a significant shift towards the harmonisation and mutual recognition of a number of qualifications, standards and licences between jurisdictions. This will help reduce the risk of identity fraud associated with mutual recognition. As business and governments develop confidence in the quality of registration and enrolment processes across Australia, these standards will also support the development of widely accepted digital identity products.

A further rationale for including registration and enrolment standards in the NISS is the risk assessment framework for enrolment standards will be more effective if it is coordinated with standards for verification and authentication.

It is important to note that the benefits of a strong enrolment framework need to be balanced with privacy concerns. In particular, agencies and private sector organisations are only to collect information that is necessary for their functions or activities.

Key achievements

A key achievement has been the development of the Gold Standard Enrolment Framework (GSEF). The GSEF specifies a best practice approach for government agencies when enrolling individuals for the purpose of issuing government documents, which may also function as key credentials for proof of identity.

While the GSEF has not yet been endorsed nationally, it does serve as the standard for the majority of key identity enrolment processes.

SECURITY STANDARDS FOR PROOF OF IDENTITY DOCUMENTS

Rationale

The majority of Australians identify themselves by physical identity credentials, such as driver licences, birth certificates, passports and citizenship certificates. While effective enrolment and registration standards create strong identity credentials, they need to be sufficiently secure to prevent their unlawful replication. Security standards for credentials

remain important for face-to-face transactions, as well as for organisations that rely on credentials as proof of identity.

A further rationale for inclusion in the NISS is that security standards need to keep pace with technological advances. This includes ease of access to sophisticated printers, which are able to produce forgeries that are difficult to detect.

Key achievements

An important achievement has been the development of the *Security Standards for Proof of Identity Documents* which has been endorsed by the Commonwealth and the States and Territories.

It specifies a best practice approach for government agencies when enrolling individuals for the purpose of issuing government documents, which may also function as key credentials for proof of identity.

THE DOCUMENT VERIFICATION SERVICE

Rationale

The Document Verification Service (DVS) was established to assist Governments to strengthen identity management mechanisms, particularly for evidence of identity process such as client enrolment. The system effectively matches the information contained an identity document (e.g. passports, driver licences) to the information held in the database of the government authority that issued the document.

The DVS is a national, real-time, on-line electronic verification system that, via secure communications links, transmits information-match requests to and match-result responses from government document-issuing authorities. The system provides a 'Yes' or 'No' answer confirming whether the identifying details contained on passports, visas, citizenship certificates, driver licences as well as birth, marriage and change of name certificates have been matched. Verifications are processed by the document's issuing authority which directly matches submitted details (document number/details, full name, date of birth etc.) against its own database.

To be most effective, the DVS requires national implementation. Unlike many countries, Australia does not have a single national identity document. Instead, Australia relies on a dispersed system of identity documents, under which individuals may use a range of identifying documents issued and managed by a range of Government agencies and non-government organisations. For this reason, an all-inclusive approach of Commonwealth and State and Territory issuing agencies for the DVS is necessary.

Key achievements

The DVS is operational, with the following agencies providing documents they issue, available for verification:

- 8 State and Territory birth certificates and change of name certificates

- 7 State and Territory marriage certificates
- 8 State and Territory driver licences
- Australian passports, and
- Australian visas, citizenship certificates, and similar immigration documents.

The Commonwealth is currently considering including Medicare cards.

To date, the following agencies have signed up to use the DVS to verify documents:

- NSW Registry of Births, Deaths and Marriages
- NSW Electoral Commission
- NSW Office of State Revenue
- NSW Roads and Maritime Services
- DFAT Passports Office
- DIAC (used for citizenship applicants)
- ATO
- Comsuper, and
- NSW Land and Property Information.

STANDARDS IN THE PROCESSING AND RECORDING OF IDENTITY DATA

Rationale

Credentials used as proof of identity reflect a person's personal details and civil status at the time the credential was issued. However, many of these details, such as name and civil status can change with time.

The agencies responsible for managing relevant registries need to have systems in place to manage this information and ensure its ongoing accuracy. The integrity of data is also important for organisations that rely on this information to verify identity. This includes regular transactions, such as accessing government benefits, and irregular transactions, such as the transfer of property.

As government agencies and business move to greater online verification of identity, the integrity of identity data stored by government agencies becomes a critical enabler for online service delivery.

Initiatives such as the DVS are reliant not only on the features of identity credentials but the integrity of the systems that issued the documents in the first place. Also, as government agencies seek to improve service delivery to customers by sharing identity information, data quality will be crucial to these initiatives.

Enhanced compatibility and interoperability across jurisdictions will improve the effectiveness of data matching. Data matching is important given the interaction of Commonwealth, State and Territory identity credentials and registers.

Improvements to the standards in processing and recording identity data are particularly important for online service delivery, by providing greater accuracy in enrolment and authentication processes. Online service delivery places the onus on government and the private sector to keep highly accurate records that are readily accessible from a number of different locations.

A further rationale for inclusion is the opportunity for jurisdictions and organisations to share approaches, lessons learned and other operational matters. This also highlights the relationship of identity data to other elements of the NISS, including the DVS.

Key achievements

Key achievements include developing a *Data Integrity Community of Practice* in the Commonwealth, and *Data-Matching Best Practice Guidelines 2009* by the Commonwealth.

Preliminary work has also begun on change of name (with further work undertaken by the Standing Council on Law and Justice), change of other details (such as sex), identity requirements for marriage, and the integrity of death data (pilot Commonwealth program).

AUTHENTICATION STANDARDS

Rationale

As the digital economy grows, opportunities for online transactions with government and private sector agencies will continue to expand. Effective and consistent frameworks for identity authentication are necessary, as identity credentials are not the only means of verifying an identity. Strong and consistently applied authentication standards will be vital for supporting any widely accepted digital identity product in Australia.

Maximising the consistency between the risk framework for enrolment and the risk framework for authentication would enhance the effectiveness of both systems. Developing common approaches to online service delivery would contribute to a seamless online national economy, and help with cross-border transactions.

Key achievements

The National e-Authentication Framework (NeAF) was endorsed by COAG in 2008.

It aims to ensure the electronic authentication (e-authentication) of the identity of individuals and business dealing with government, as well as the authentication of government websites.

The NeAF uses a set of operating principles and relies on a risk-mitigation approach. It allocates the consequence of misuse into one of five categories, and then applies one of four levels of authentication to respond to that risk.

BIOMETRIC INTEROPERABILITY

Rationale

As identifiers, biometrics must be considered in an identity management context, where the strength of initial enrolment processes determines the level of trust for future transactions.

Biometric interoperability relates to establishing conditions so agencies can share data, match against legacy data, or cross-reference data. Interoperability relates to the adoption of common standards, along with a coherent and consistent use and management of, biometric information across jurisdictions.

The misuse or abuse of a single biometric may have severe implications for the individual to whom it relates, and any biometric system with which it is used or matched.

Key achievements

Work has been undertaken by individual jurisdictions, such as the use of facial recognition technology by NSW Roads and Maritime Services.

The Commonwealth has started exploring interoperability across Commonwealth government agencies, to develop a joint approach to collection, sharing, storage and capability development for biometrics.

GOALS TO GUIDE THE NISS

The following goals will help guide future work under the NISS.

It is important to note that the goals are aspirational and the work to address them will proceed at different levels among jurisdictions. This is due to a variety of reasons, including available resources and competing priorities.

REGISTRATION AND ENROLMENT STANDARDS

- where the risk requires, apply the GSEF in a consistent fashion nationally, particularly when issuing identity credentials and making transactions that are too sensitive to be conducted online
- work towards consolidating and measuring evidence from service delivery agencies, to determine the incidences of each kind of credential being exploited as part of identity crime and misuse
- work towards consolidating and measuring evidence from service delivery agencies and law enforcement bodies, to determine whether standards are being applied consistently
- work towards consolidating and measuring evidence from service delivery agencies and law enforcement bodies, to determine the extent to which people are experiencing barriers to service delivery because identity credentials that were subject to the GSEF are not being accepted by particular agencies
- determine the requirement for a 'silver standard' enrolment framework to be used when the immediate and downstream risks for enrolment are lower than the threshold for Gold Standard Enrolment

SECURITY STANDARDS FOR PROOF OF IDENTITY DOCUMENTS

- maintain and continue to strengthen commonly used credentials (including the standards underpinning the credentials), according to their value to society
- maintain and continue to examine enhanced security measures associated with credentials, in line with technological challenges and opportunities
- work towards consolidating and measuring evidence from service delivery and law enforcement agencies about the prevalence of fraudulent identity credentials, their links to other criminal activities, and the means by which the counterfeits were detected

THE DOCUMENT VERIFICATION SERVICE

- consolidate and expand the use of the DVS by jurisdictions
- examine opportunities to expand the use of the DVS

STANDARDS IN THE PROCESSING AND RECORDING OF IDENTITY DATA

- improve interoperability and data-matching, within the confines of existing privacy laws and best practice
- work towards improving data-matching techniques and examining the benefits of data-matching for agencies

- assess the risks associated with the abuse of vulnerable identities by criminals, and the development of appropriate mitigations

AUTHENTICATION STANDARDS

- review the validity of current e-authentication frameworks on a risk basis
- work towards applying e-authentication standards consistently across jurisdictions

BIOMETRIC INTEROPERABILITY

- develop a national biometrics interoperability framework
- ensure that biometric practices across governments, the private sector and the community in general, protect privacy while enhancing service delivery

EVIDENCE BASE AND MEASUREMENT FRAMEWORK FOR IDENTITY CRIME AND MISUSE

- progress a national framework to provide an ongoing collection and analysis of identity crime and misuse information, that will allow longitudinal reporting on such activity in Australia
- source data from relevant Commonwealth agencies to initially scope, develop and populate the indicators and narratives
- explore expansion of data collection to State and Territory governments and industry bodies

SUPPORTING THE AUSTRALIAN PUBLIC TO PROTECT AND RESTORE THEIR IDENTITY

- enhance collaboration between Commonwealth, State and Territory government agencies to help victims of identity crime recover their identities
- examine closer collaboration between business and government agencies to help victims of identity crime recover their identities
- through appropriate support, help the most vulnerable Australians to prevent their identities from being exploited, focussing particularly on Commonwealth identity credentials
- develop collaboratively, consistent education and awareness raising messages about identity security for the public
- help the public access existing identity security information (that is demographically and culturally appropriate), to enable informed risk-based decisions about protecting their own identity information
- support small to medium business in understanding the risks to their customers of storing too much information, and how to minimise collection and storage of identity information.

IMPLEMENTING THE NISS – 2012 ONWARDS

In the course of reviewing the NISS, jurisdictions came to the following conclusions:

- the NISCG be retained as the primary vehicle for inter-jurisdictional collaboration and information exchange
- the six elements of the NISS remain relevant in today's identity security environment
- where practical, the six elements of the NISS are supported by a range of initiatives that sit across all aspects of identity security. In particular, jurisdictions will place greater emphasis on:
    - the collection and measurement of evidence, particularly in relation to the incidence of identity crime and misuse, and
    - educating the Australian public (particularly individuals and small to medium business) about how to protect their own (and each other's) identity information
- where a risk has been identified, particular attention needs to be given to supporting Australians who have become, or who are at risk of becoming, victims of identity crime.

THE NISS WORK PLAN

To implement the revised NISS, jurisdictions will develop a work plan on an annual basis. Each work plan will be developed by the NISCG separately to this document.

Collectively, the annual work plans will form a living document. It will be updated in response to evidence-based risks and opportunities, as well as attempting to address long standing barriers to implementing existing work.

Jurisdictions will determine which activities will address strategic outcomes of national significance, with a strong emphasis on providing a forum to identify and reduce barriers.

The work plan will improve each jurisdiction's accountability to COAG, by including a lead agency's deliverables and timelines to each activity. This accountability will be reinforced as the NISCG reports to COAG annually on the achievements of work plans.

Work undertaken on a national level:

The each annual work plan will identify priority issues that require national attention.

Work undertaken on a jurisdictional level to achieve a national outcome:

In recognition that different jurisdictions have implemented elements of the NISS to varying degrees, the work plans may also identify areas where two or more jurisdictions can cooperate to consistently implement work that may be more advanced in other jurisdictions.

NEW BENEFITS AND OPPORTUNITIES THE NISS CAN HELP DELIVER

Since work on implementing the 2007 NISS began, consumers have embraced the opportunity to interact with government and business, particularly online. The growth of online services has the capacity to deliver significant benefits to governments, business and the community.

Benefits to government

- a nationally consistent approach to identity security will help create an expanded national digital economy – reducing inconsistencies between jurisdictions and promoting confidence in information used to register for government services
- greater opportunities for governments to provide services and transactions online
- protection of public revenue and private assets through reduced fraud and error
- support for law enforcement and national security agencies, as they seek to make it harder for criminals and terrorist groups to operate in Australia

Benefits to business

- business will also benefit from a national approach to identity management and an expanded national digital economy, by reducing regulatory complexity and contributing to a seamless national economy
- reduced risk of fraudulent and mistaken transactions through enhanced identification processes, and ongoing work on data quality and accuracy
- business confidence in the integrity of identity management in Australia will help with productivity by allowing business to trust the identity of customers with minimal verification
- opportunities to streamline compliance with legislative obligations relating to proof of identity, through enhanced verification and authentication procedures

Benefits to the community

- enhanced privacy for users, arising from efficient validation and verification processes
- enhanced trust in identity data, promoting community engagement in the digital economy
- enhanced in-person transactions by using efficient systems and prioritising transactions that require in-person verification
- reduced risk to individuals of becoming a victim of identity crime.

LESSONS LEARNED

Along with the achievements of the NISS to date, the Commonwealth, State and Territory governments learned important lessons about what needs to happen next, and how to improve existing efforts in identity security. These are outlined below.

Review of the intergovernmental agreement

The review concluded that the current IGA on identity security remain as is, and be re-affirmed by COAG.

The IGA allows for the good work of the NISS to continue, while also having the capacity to be built upon, as the parties to the Agreement learn more about how best to tackle challenges and opportunities.

Strategic direction

The review concluded that the NISS has been effective in initiating valuable work on identity security in Australia.

It also concluded that high level outcomes and guiding principles would also be a valuable inclusion in the NISS. A clearly articulated approach to identity security will enable all jurisdictions to respond to emerging challenges and opportunities in a consistent way. In addition, strategic guidance will allow jurisdictions to be proactive about the future of identity security in Australia, rather than responding only to current pressures and opportunities.

As such, the Commonwealth, State and Territory governments have developed the NISS 2012 for COAG to endorse.

RECOMMENDATIONS

Based on the review, jurisdictions recommend that COAG:

1. **agree** to adopt the strategy outlined in *NISS 2012* and the *Work Plan for the National Identity Security Strategy FY2012-13* developed to commence implementation of the 'Goals to guide the NISS' as described in this report (pages 8-9).