National Identity Security Strategy **2012**

IDENTITY SECURITY

ISBN: 978-1-922032-03-4

Use of the Coat of Arms

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Business Law Branch
Attorney-General’s Department
3–5 National Cct
BARTON ACT 2600
Telephone: 02 6141 6666
copyright@ag.gov.au

Table of contents

Executive summary

The Commonwealth, State and Territory governments are committed to helping ensure that Australians may confidently enjoy the benefits of a secure and protected identity.

A secure identity system in Australia is an essential element for most business transactions. Moreover, a secure identity system enables better government service delivery, particularly online. Good identity security also enhances privacy as it helps to stop unauthorised access to personal information.

Identity security plays an important role in preventing serious and organised crime, as well as terrorist activities. Identity theft and misuse allows criminals to mask their true identities, or create false identities, so they can perpetrate crimes undetected. Identity theft is a costly experience for the victim, and also potentially damaging to their financial and personal reputation.

In 2007, the Council of Australian Governments agreed to the National Identity Security Strategy (NISS). Since then, the NISS has advanced the cause of identity security substantially. Key achievements include the establishment of the Document Verification Service and the development of several national standards related to identity management.

In a review of the NISS, the National Identity Security Coordination Group concluded that the strategic direction of the NISS required greater clarity about how best to respond to identity management challenges and opportunities. This document seeks to fulfil that aim by including the following guiding principles.

- Protecting the identity information of Australians is a shared responsibility
- The community's confidence in business and public trust in government is supported by identity security
- To deter crime and foster national security, identity security must be based on a risk management approach
- Commonly accepted identity credentials must be supported by strong security measures, and
- Identity security needs to be a core feature of standard business processes and systems.

The guiding principles are consistent with the following policy objectives, as agreed by the Commonwealth, State and Territory governments: that identity security measures not only PREVENT and DETER crime but also help DETECT and MEASURE incidences of crime. Moreover, these security measures should ENABLE the digital economy and help victims RECOVER their identities.

As such, all governments will work towards achieving the following goals.

- Maintain their focus on developing and implementing national standards across a range of identity related processes.
- Continue enhancing and expanding the Document Verification Service.
- Focus on taking advantage of the benefits and addressing the challenges of biometric technology.
- Improve the quality and consistency of the evidence of identity crime and misuse, to improve responses to these challenges.
- Look at ways to support the Australian public, so they can protect themselves and if necessary, restore their identity.

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.*

Scope and background

What is identity security? It is the security of who a person is, or the evidence a person uses to prove who they are.

Identity security is a balancing act between:

- protecting a person's identity information from being stolen, duplicated or misused (confidentiality)
- keeping a person's identity information correct (integrity), and
- making sure the right people have the right level of access to the identity information (accessibility).

The scope of the NISS is shaped by the need to

- strengthen national security
- prevent crime, and
- enable the benefits of the digital economy.

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.

A nationally consistent approach is vital to ensuring a high degree of identity security. Increasingly, documents and identity details issued and stored by the private sector (such as credit cards and email addresses) are being used as identity credentials in both online and offline commerce. Over time, the private sector will share a greater proportion of the responsibility for Australia's identity security.

What is the difference between identity security and identity management?

Identity management looks at how identity information is collected, stored and used in order to support a business process.

Identity security addresses the risks associated with legitimate management practices in order to protect people's information and maintain the integrity of the business process.

It was at a special meeting on Counter-Terrorism on 27 September 2005, that the Council of Australian Governments agreed to develop and implement a NISS by way of an Intergovernmental Agreement (IGA).

The 2007 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.

A review of the IGA was conducted in 2012. It concluded that:

- the IGA should continue to support Australian governments working together to achieve the objectives of a revised NISS
- there is still important work to be done against each of the elements of the 2007 NISS, while also focusing on new dimensions
- there is a need for greater clarity around the strategic direction of the NISS in order to help deliver a more consistent and proactive national approach to identity security – one that will prepare Australia for future opportunities and challenges, and cope with the changing digital and technological environment
- including policy objectives and guiding principles would help shape, guide and enhance the work of the 2007 NISS, so that the Australian community is better placed to face and overcome future challenges in identity security.

Each of the above findings has been incorporated in developing the 2012 NISS (this strategy).

Overall objective

The key outcomes of this strategy are to enhance national consistency and interoperability (eg the ability of different computer systems to share data and work together).

The overall objective of this strategy is to:

> *work collaboratively with the Commonwealth, States and Territories to enhance national security, combat crime and enhance opportunity (including for government service delivery) through nationally consistent processes for enrolling, securing, verifying and authenticating identities and identity credentials.*

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. Good identity security enhances the capacity for us to engage with each other more securely in a range of different ways, including online.

For governments, a national approach to identity security reduces inconsistencies between jurisdictions and promotes confidence in the information used to register for government services. This capacity is fundamental to realising the cost savings that come with providing services and transactions online, as well as protecting public revenue and private assets through reduced fraud and error. The NISS also provides an excellent opportunity for jurisdictions to share lessons learned, develop interoperability and other collaborative activities that not only strengthens Australia's identity system but can lead to more cost-effective security measures.

Apart from the benefits to governments, good identity security also helps business by reducing regulatory complexity and contributing to a seamless national economy.

For individuals, good identity security enhances every person's capacity to control their private information and have greater confidence in transacting safely online.

Growing threats & challenges for the NISS to address

While the digital economy provides new opportunities and benefits, it has also given rise to significant threats that governments need to address, in partnership with business and the wider community. Identity related crime continues to be a significant concern.

While there is no definitive cost of identity crime, it does have many victims.

A 2007 Australian Bureau of Statistics survey on *Personal Fraud* reported that almost 500,000 Australians were victims of identity theft and credit/debit card fraud [1].

In 2012, the Commonwealth Attorney-General's Department conducted a survey on *Identity Theft*. It showed that 7% of Australians had been a victim of identity theft or misuse in the preceding six months[2].

This problem is not restricted to Australia. In the 2008 *Scoping Paper on Online Identity Theft*, the OECD reported that identity fraud in the United Kingdom costs £1.7b annually. The OECD also cites figures that in 2007, the cost to industry and consumers in the United States was US $49.3b.

In addition to direct costs, identity theft and identity fraud also enable other criminal activity. This is partly because identity information provides access to other forms of financial benefits, including access to government benefits and credit facilities.

In the report *Organised Crime in Australia 2011*, the Australian Crime Commission determined identity theft as a key enabler for organised crime. The report also noted that serious and organised crime is estimated to cost Australia between 10 to 15 billion dollars each year. Identity theft and false identities remain the key enablers of superannuation fraud, particularly involving criminal access to an unwitting beneficiary's superannuation account[3].

As is the case internationally[4], most identity crime is not reported to law enforcement agencies. This is either because victims are not aware their identity has been stolen, or because they choose not to report it. The under reporting of losses incurred by financial institutions impedes assessment of the extent and scope of identity crime and costs against this sector. Under reporting also impedes the ability of law enforcement agencies to investigate identity crime[5].

The increased reliance on personal identification over a wide range of transactions in both public and private sectors[6] has made the Australian community highly vulnerable to misuse of identities and fraudulent practices (ATM vulnerabilities, insider recruitment, data warehousing and 'card not present' fraud).

[1] Australian Bureau of Statistics (ABS) 2008, *Personal fraud 2007*, Cat. No. 4528.0. Canberra: ABS, pg 7

[2] Attorney-General's Department (2012) *Identity Theft: Concerns and Experiences*

[3] Australian Crime Commission, *Organised Crime in Australia 2011* at pg 78

[4] Hoofnagle, C.J. Identity Theft: making the known unknowns known, Harvard Journal of Law and Technology: 21(1), 2007

[5] The Growing Global Threat of Economic and Cyber Crime, The United States National Fraud Centre, December 2010, pg 29

[6] M. Yip, *School of Engineering and Computer Science, University of Southampton* identified that social networking is a critical process for the profit seeking cybercriminals, in his article *An Investigation into Chinese Cybercrime and the Applicability of Social Network Analysis* (available from author)

Harm caused by these crimes includes large financial losses for victims, who may also have to restore their tainted identity, including their reputation and position in society at large. International research has found that the growing incidence of identity theft and identity fraud has also had a detrimental effect on e-commerce[7].

Increasingly, identity crime and misuse is being supported by specialised criminals using sophisticated techniques to either manufacture or obtain identity documents or information. The increasing specialisation of such crimes indicates there is more profit to be made from this pursuit than in the past.

Identity security measures have become more successful in protecting the Australian community and deterring identity related fraud. However, this has had the unwelcome side effect of shifting the focus of fraud away from the identity credential itself, to achieving fraud through an assumed identity.

If an offender is able to misrepresent themselves with a bogus identity credential during the application process of another identity credential, then detection of the original fraud becomes extremely difficult[8].

These growing threats reveal a range of vulnerabilities, especially in the:

- ability to measure identity crime and misuse and then determine the effectiveness of identity security policy and practice across Australia
- capacity to withstand the increasingly sophisticated method of accessing or interfering with identity data, and
- capacity to help individuals recover their identities from theft or loss.

[7] *Measuring identity theft and identity fraud,* Int. J. Business Governance and Ethics, Vol 5, Nos. 1& 2, 2010 at pg 62

[8] International Civil Aviation Organisation, *Towards Better Practice in National Identity Management,* pg 1

The direction of the NISS

To maintain a common direction for all Australian governments, and to address the weaknesses and opportunities in our national system of identity, this strategy includes five guiding principles.

These principles highlight best practice for identity security. They aim to create a clear understanding of Australia's identity security environment, and how identity security measures need to be designed.

Guiding principles

PRINCIPLE 1 – protecting the identity information of Australians is a shared responsibility

Identity crime and misuse is a cross-border activity. It operates on a national and international scale – and will exploit weaknesses in one jurisdiction to obtain benefits in another. This is particularly relevant in Australia, where individuals build their identity with a combination of credentials. These credentials can be issued by multiple jurisdictions, and are often mutually recognised.

Jurisdictions have a mutual reliance on the integrity of each other's identity security frameworks. If one jurisdiction has a less rigorous framework for allocating an identity credential, then it can be exploited.

Once an identity credential has been issued from a jurisdiction with a less rigorous framework, it can be used to establish financial services accounts, utilities accounts and other services. These accounts and services can then be used to obtain government services, or establish an identity in a jurisdiction with a stronger identity security framework. This is why a cooperative approach between jurisdictions is required.

While individuals have the primary responsibility for their own identity, it is not feasible for individuals to have complete control over their identity information. It is governments and the private sector that must share the responsibility to protect that information.

Each government agency needs to consider how their security risks, particularly around accepting or issuing identity credentials, may affect the rest of the Australian community.

Likewise, business and not-for-profit organisations hold large amounts of identity information, and make identity security risk assessments that have downstream consequences. They are also targets of identity crime and misuse, and need to consider the impacts of a security breach on their reputation and the Australian community.

It is also important that information regarding system breaches and identity thefts are collated and made available to the community in an appropriate format. This will help mitigate further losses and help with re-establishing compromised identities.

PRINCIPLE 2 – the community's confidence in business and public trust in government is supported by identity security

It is important for Australians to be confident that business and government share the responsibility for protecting their identity information (as per Principle 1).

For example, Australians need to provide personal information to some government agencies to participate in society. In turn, Australians must be able to trust that government agencies are supporting and enhancing their privacy.

Government agencies are improving the delivery of face-to-face and online services to the community. A good reputation for service delivery and privacy is developed over time, through public trust that proper security measures are in place. Well integrated, seamless identity security measures are more difficult to by-pass and are a less attractive target for criminals. They also reduce the time and effort required by individuals to verify their identities.

A good reputation for security is also developed through proper disclosure of system breaches if they occur. Over the long term, this allows people to be confident that the absence of reported breaches is a positive sign.

It is therefore important that business and government address their identity security vulnerabilities through proper risk assessments (as per Principle 3).

PRINCIPLE 3 – to deter crime and foster national security, identity security must be based on a risk management approach

Good risk management is an ongoing process. It involves establishing a context, determining threats, vulnerabilities and criticality, then analysing likelihood and consequence before evaluating and treating significant risks .

Key to any risk assessment is an appreciation of how a threat or vulnerability will affect the confidentiality, integrity or availability of identity information.

Governments need to make sure they work together to prevent threats to individuals. This is more likely to be achieved when governments contribute to measurement frameworks that assess the effectiveness of the steps they take to prevent crime and terrorist activity, as well as implementing lessons learned.

Anonymity vs. verified identities

If identity security risk is negligible to all parties, an individual should be able to remain anonymous or use a pseudonym if they choose. However, if risks to one of the parties are unacceptable, the identity of the other party must be confirmed. For government agencies, unacceptable risks include those that may lead to identity crime.

Identity crime is a significant threat to Australia's national security. This is not only because of its immediate impacts on the individual victims but because the misuse of identity can facilitate other, often more significant criminal activity, including organised crime and terrorism.

Integrated and risk-based identity security measures reduce the likelihood of identity information being misused. These include strong credentials and authentication measures, thorough document verification, and techniques to improve data integrity, such as data-matching. Putting these measures in place reduces systemic vulnerabilities and enhances the integrity of systems that may otherwise be exploited by criminals.

[9] International Standardization Organization - Risk management - Principles and guidelines ISO 31000:2009

How much identity information is needed?

It is important for individuals to be confident that a government agency, business, or not-for-profit organisation, will not collect more identity information than is necessary or appropriate.

In general, the various privacy laws in Australia provide that a government agency or a large organisation is in breach of the law if it collects more information than necessary. However, it is the responsibility of each government agency to determine the minimum level of information according to operational requirements.

This decision depends, in part, on the identity security measures in place. Effective identity security measures can potentially reduce the amount of personal information an agency requires.

A security risk assessment can help identify how much identity information might be needed. Collecting too much information can incur costs and increase risks to an organisation, just as much as collecting too little. In some cases, an assessment of the minimum level of required information will need to consider interoperability and legislation, such as the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006’*.

PRINCIPLE 4 – commonly accepted identity credentials must be supported by strong security measures

Various documents and electronic forms of information (e.g. online usernames and passwords) are gaining credibility as acceptable identity credentials, even if that was not their original purpose.

Issuing agencies need to be aware of the extent to which a document or an electronic form of information is being presented – and accepted – as proof of identity in the wider community.

Key questions for issuing agencies are:

What are people choosing to use as an identity credential?

What documents are being required for a process of identification?

Over time, the types of documents and electronic information that are used and accepted as proof of identity will change, particularly as the contents of people's wallets move from being in hard copy to being online. Jurisdictions and their agencies need to consider these changes as part of their regular risk assessment updates.

Issuing a strong identity credential

Issuing agencies need to ensure that the security of their credentials can be compared and contrasted with similar credentials. Adopting common security standards will provide the kind of transparency that the Australian community can rely on.

Government agencies issuing credentials, especially foundation identity documents (e.g. passports and drivers licences), need to be aware of how their credentials are being used in society, and the downstream consequences of their security decisions.

PRINCIPLE 5 – identity security needs to be a core feature of standard business processes and systems

Identity security measures are a cost of doing business. However, well considered identity security that is properly integrated into business systems, is ultimately less expensive than security systems included later.

When security is one of the final considerations in system design, it can result in an extra layer of not only cost but complexity. It can also leave the whole system exposed.

It is also important to allow for system integrity checking across agencies. This means reporting and information sharing mechanisms also need to be built into the design of identity management systems.

Policy objectives

While the guiding principles outlined above highlight best practice for identity security, it is important that continued improvements are made to identity security in government agencies. These improvements are needed to support innovation and efficiency, especially as we move to a greater reliance on the digital economy.

The guiding principles are also consistent with the following policy objectives, which show what Australian governments are seeking to achieve in identity security. These objectives support law enforcement, national security, and government service delivery outcomes.

OBJECTIVE 1 – PREVENT and DETER identity crime and misuse

Australian governments are committed to developing policy and programs that prevent and deter identity crime and misuse. This is a complex problem requiring an integrated response across all jurisdictions – and with the whole community.

There is no one solution and no one agency or organisation that can prevent identity crime and misuse. Prevention requires well considered measures at every step of the identification process, to ensure a credential is linked to the right person.

Deterrence is an outcome of preventative measures. As it becomes harder for criminals to steal or misuse identity information, some will move to easier or less resource intensive forms of crime.

OBJECTIVE 2 – DETECT and MEASURE identity crime and misuse

Due to its nature as an enabler of other serious forms of crime, identity crime and misuse often goes undetected or unmeasured.

Improving the capacity to detect and measure identity crime and misuse, will also improve efforts to prevent and deter identity crime and misuse.

OBJECTIVE 3 – support Australians RECOVERING from identity theft or loss

The ability of an individual to credibly demonstrate their identity is vital for participating in Australian society.

However, for individuals who have lost identity documentation, it can be extremely difficult to meet strict requirements to establish their claimed identity with any confidence. It is therefore important that appropriate support is provided to individuals who have experienced identity theft or loss.

OBJECTIVE 4 – ENABLE trusted online business and interactions through stronger identity security

Identity security, like cyber security, is a vital element of the digital economy.

Governments, business and individuals are increasingly taking advantage of trusted online interactions. It is therefore important that the Australian community has as much confidence in the identity credentials presented online, as they do in identity credentials presented in hard copy.

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 Gold Standard Enrolment Framework (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 and law enforcement bodies , 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 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 developing appropriate mitigations

Authentication standards

- review the 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 government agencies 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.

Key policy links

To maximise the effectiveness of the NISS, it needs to be consistent with other areas of public policy, as outlined below.

Identity security and cyberspace

The Australian Government released its Cyber Security Strategy (CSS) in 2009. Its aim is *the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy.*

The CSS and the NISS both aim to maximise the opportunities of the digital economy, so there will be links between them. For example, the steps needed to authenticate online transactions.

The Commonwealth is also developing a white paper, which will review how governments, business and individuals can realise the full benefits of cyberspace, while managing current and emerging risks.

It will be important to ensure the work of the NISS effectively leverages off the implementation of these wider policy outcomes, and that effective identity security measures are elements of these outcomes.

Identity security and consumer protection

There is a strong connection between identity theft, identity fraud and other forms of fraudulent conduct, such as superannuation fraud.

Jurisdictions need to look at establishing networks with relevant consumer protection areas of government, particularly in relation to public messaging, to explain the risks associated with identity fraud and the long term implications of identity theft.

Identity security and privacy

Information used to establish, verify or authenticate identity will often fall under the regulation of Commonwealth, State and Territory privacy laws and policies.

An overly regulated identity security regime would be harmful to privacy if it required excessive disclosure or exchange of personal information for a transaction that has minimal risk of fraud or other misuse. Rather, effective identity security would enhance privacy by protecting people's identity information from theft or misuse.

Work already done under the NISS has aimed to strike a balance between enhancing identity security, while ensuring an appropriate consideration of privacy. Further work needs to continue pursuing this balance.

NATIONAL IDENTITY SECURITY STRATEGY

IDENTITY SECURITY