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

Report – March 2019

Roger Wilkins AO and Professor David Lacey.

"What is the name of your first pet?"

This document does not reflect the official views of the Department of Home Affairs. The contents of this report represent the views of Roger Wilkins AO and Prof David Lacey, the Review's independent leads.

Important Note:

This report has limited distribution and is NOT to be disseminated further in whole, or in part. If you would like to discuss any aspects of this document, or have any questions on the Review of the National Arrangements for the Protection and Management of Identity Information, please contact the Review team; s. 47E(d)

Contents

Executive Summary

The current "system of identity" in Australia has grown up in an ad hoc way. It has a large number of weaknesses and deficiencies. Compared with a number of other countries, Australia's "system" of identity is more costly, inconvenient and less secure. It is certainly more costly, inconvenient and less secure than it should and could be. It is not a system that is fit for a future in which transactions will be largely carried out online. Police, crime commissions, businesses and government agencies have all advised that fraud and identity "theft" are increasing at a concerning rate.

The current "system of identity" is also uneconomical with identity data. A lot of information is collected and retained for "identity proofing" by a lot of different businesses and agencies. This is not good for privacy or security.

Citizens and consumers have an ever growing number of credentials with complex access requirements, and even more complex and time consuming processes for restoration in the event of "loss" or compromise.

The "system of identity" is not difficult to reform so that it would be much easier to use and much more secure. Indeed, there are a variety of reforms "in the pipeline". These are not particularly well coordinated, and they do not have the impetus and commitment needed.

This report sets out a framework for the reform and maintenance of the system of identity in Australia.

All Australian citizens and residents should have a "core credential" that is biometrically based which they can use to prove their "identity".

These "core credentials" already largely exist. They include passports, driver licences, ImmiCards and Proof of Identity cards. It is just that not everyone has one of these and they are not all "proofed" to a high standard.

Facial biometrics are central to reform of the system of identity. Facial biometrics are intimately tied up with our idea of "skinny identity". All that is needed for a person to identify themselves is a biometric, a name and date of birth, provided these have been proofed to a high standard. No other data or information should be required.

A citizen or consumer can prove their identity to a business or government agency or organisation simply by using a "core credential" with a biometric. The business or government agency or organisation only needs to check the "core credential" and the biometric with the Document Verification Service (DVS) and the new Face Verification Service (FVS) to ensure that it is genuine. There is no need for the business, government agency or organisation to collect and retain the biometric information.

We call this a "system of reliance" where businesses, governments, citizens and consumers "rely" on a small number of core credentials which embody a "skinny identity".

Businesses and organisations may want to rely on the core credential and then issue their own credential. Similarly, governments many want to rely on a core credential and issue a digital ID.

The system of reliance on core credentials does not prescribe all the ways in which it can be used. But it does say that citizen's "consent" or "control" should govern its use. The system essentially provides a foundation for identity.

The key things that need to be done to implement this system are set out in the Report. They include:

1) Institute a new high standard of "proofing" identity for the purpose of issuing a core credential. Mostly this will impact on driver licences; Passports already meet this standard. There is already an agreement by governments to do this.
2) Complete the Face Verification Service (FVS) and make it available to the private sector. This is being piloted at present.
3) Make sure that all Australian citizens are able to get a core credential. This means that the Australian Passport Office (APO), Driver Licence Agencies (DLAs) and the

Department of Home Affairs (Home Affairs) should be able to offer Proof of Identity credentials to people who have no need to drive or travel.

4) There are a significant number of people who do not have the documentation necessary to prove their identity. These people are most often clients of the Department of Human Services (DHS). DHS should put in place a program to provide these vulnerable clients with Proof of Identity Credentials.
5) Put in place an "Identity Code" that goes further than the current "proofing guidelines" in setting out not only standards for proofing identity but also rules and norms for maintenance, restoration of identity and the right (and obligations) of citizens, government agencies and businesses in relation to identity management.

Perhaps the most critical recommendation is a piece of institutional reform. There is currently no one in the system who has overall responsibility for identity policy and practice. There are many "players" at a Commonwealth, State and Territory level but no agency responsible for the overall "health" and functioning of the "system".

It is fundamental to the reforms we advocate that there should be an "Office of Identity Protection and Management" (OIPM) that has four main functions:

- Establish and publicise the rules and standards that "govern" identity in Australia
- Ensure compliance with these rules and standards
- Deal with complaints and problems, or at least make sure they are dealt with by the right person or agency.
- Identify/anticipate emerging problems and trends and keep the system under review, and institute changes where necessary.

The OIPM should be a "national agency". The Commonwealth should set it up (probably as part of Home Affairs). It should include State and Territory secondees (and perhaps the private sector as well on the model of the FINTEL Alliance in AUSTRAC).

Another key institutional arrangement is to embody key recommendations of this report in a "National Strategy on Identity" that would be agreed between all governments at the Council of Australian Governments (COAG).

There are a large number of reports to government over recent years that have called for these sorts of changes to the system of identity.

These include David Murray's report on the financial system in Australia, and most recently the report to the Commonwealth Government by the "Black Economy Taskforce". Internationally, bodies such as the World Bank, United Nations, and Financial Action Task Force (FATF) have advocated these types of reforms.

The reforms are not all that radical or dramatic. Indeed, many of the changes required are already agreed to. What is needed is better coordination, greater impetus, political will and resources, both people and money.

The reforms advocated here have three significant benefits for Australia:

First, the reforms constitute a significant fraud and crime prevention measure. A weak system of identity is used by criminals and terrorists to compromise and "steal" identities to defraud people and commit crimes.

Second, the reforms constitute a significant efficiency for citizens and consumers in obtaining goods and services from government and the private sector. Particularly with the increase of online transactions, the changes we advocate should render transactions and dealings simpler, easier and more secure.

Third, the interoperability and mutual recognition of identity is an important micro-economic reform. For example, greater ease of consumer choice in the financial sector, the energy sector, the telecommunications sector, presupposes a secure and efficient identity credential easily transferred and accepted by different providers.

1. What is the "problem of identity" we are trying to solve?

The problem of identity is essentially a product of technological, social and economic change. More and more of our dealings with people are now remote, transitory and relatively anonymous.

Historically most transactions and relationships tended to be physically proximate, involving face-to-face dealings, and very often repeat contacts and transactions. Social and economic networks were local, or, to use Robert Putnam's terminology, exhibited a high degree of "social capital". Organisations like guilds, professions, chambers of commerce, banking, insurance, and trade tended to operate as "clubs" that "vetted" and "vouched" for their members.

These structures and practices have broken down under the pressure of technological, social and economic change. The greater mobility of people, capital and goods and the emergence of more complex and differentiated economies and societies, has meant that transactions and relationships are more "remote" and "anonymous".

"Proving" one's identity is now a normal part of the way we live and is a necessary precondition for accessing all sorts of goods and services and assets. This is especially so for online transactions. People now need to concern themselves with their own and other people's identity on a regular basis.

How certain anyone needs to be about the identity of another person depends on two things. First, how significant are the consequences of being wrong? Is there a lot or a little at stake? The second thing is, how likely is it that we are wrong about the person's identity? How secure are our grounds for believing that the person is who he or she claims to be.

"Proving" identity is becoming a more and more important issue for a range of reasons.

First, sorting out a robust way of proving identity is a critical crime prevention measure. It is a way of protecting people's rights, entitlements and assets from being stolen or misappropriated.

Second, a robust system of identity proofing is a critical factor in the delivery of goods and services by government and businesses. This is particularly the case for online transactions.

Third, a robust system of identity proofing should also be seen as "critical" infrastructure that creates opportunities for innovation, productivity and broader economic development. Examples of that include things like open banking, peer-to-peer lending, Uber and Airbnb.

2. What is identity?

We define an “identifying attribute” or “characteristic” of a person as an attribute or characteristic that is peculiar or unique to that person; that distinguishes that person from other people.

An identifying attribute or characteristic need not tell us a lot about a person, about their history or background or relationships. Physical properties like fingerprints or a person’s face or iris for example, do not carry much information about what a person is like or what they have done etc.

What identifying attributes or characteristics need to do is enable a person to differentiate herself/himself from other people and to demonstrate that he or she is the same person at different points in time.

3. A “skinny” concept of identity

David Hume was interested in the notion of “personal identity” because he was interested in the essence of “personhood”. He wanted to escape from the idea that what made a person distinct and different had to do with a “soul” or “mind” or some sort of “spiritual substance”. He thought that what constitutes “personal identity” has to do with the continuity and coherence of the history of the person. The actions and relationships of a person over their life. What makes the baby the “same person” as the old man is a single, coherent history that leads from one to the other.

Hume’s philosophical problem will not concern us in this report, but his account does have an affinity with a view of identity that sees an identity as having to do with a person’s “social footprint” – a person’s activities, dealings and relationships. Rather like Hume, advocates of this view say that establishing a person’s identity is about establishing a coherent and consistent history of the person.

We do not advocate this approach. We describe it as a “fat” concept of identity, because it requires us to know a lot of things about a person to establish their identity. We prefer what we call a “skinny” concept of identity that requires us to know only about some unique physical characteristics of a person to identify him or her (a “biometric” characteristic or attribute), as well as a limited number of other attributes such as name and date of birth.

We advocate this “skinny” concept of identity for a number of reasons.

As the terms “fat” and “skinny” suggest, biometric attributes carry very little information about the person. If we want to maximise privacy then we should prefer this “skinny” concept.

A “skinny” identity is generally easier to establish and use. It is difficult to misplace, lose or steal a person’s biometric attributes.

A “skinny” identity is fungible and portable. Biometric attributes are physical properties shared by all human beings no matter where they are, and a number of international bodies are looking at biometric attributes as the key to international interoperability.

Biometrics are already being used in Australia for a number of identity documents – passports, some driver licences, some working with children cards, some gun licences. Australians also use biometrics to operate smart phones and computers and to access services such as banking, communications, and accommodation.

In our view the use of biometrics is at least as important as developments such as the internet in transforming the ease and reliability and security of carrying out everyday activities and dealing with business and government.

4. An Identity System

4.1 What is an identity system?

In this section we are concerned with the "structure" or "logic" of a system of identity. It is easiest to think of a system of identity as a sequence of processes.

"Establishing a person's identity" or "identity proofing" is the foundation of an identity system. Indeed some people talk about a "foundational identity"[1] . Essentially, this is a process defining those attributes or properties or events that are going to constitute the person's identity in the system. We argued previously for a "skinny" concept of identity. We would opt for a small number of attributes – biometric properties, a name, maybe date of birth. We will call this the person's "core identity".

"Verification" of a person's identity is a process of determining whether a person is the person they claim to be. This person claims to be Roger Wilkins. Does he have the fundamental attributes that constitute Roger Wilkins's core identity? Typically, this is a process that relies on foundational documents such as a passport, driver licence, birth certificate, visa or maybe a citizenship certificate.

Typically this is a threshold process for "on-boarding" a person for example, as a bank customer, a tax payer, a telco consumer, a social security client etc. Typically, it also makes use of documents or evidence of identity by checking these through the Document Verification System (DVS) or Face Verification System (FVS).

Typically, when a person's identity has been verified in this way, he or she is given a "credential" or "method of proof" that they can use for subsequent transactions or access to the goods or services.

[1] *The World Bank Group*, G20 Digital Identity Onboarding, Argentina 2018

"Authentication" of identity is a process where the person's identity is checked before they are permitted access to goods, services or assets. Typically the person uses the credential given previously when he or she was on-boarded and verified.

"Maintenance" of identity is not really a discrete process. The following processes could be included in the list of things that constitute "maintenance of identity":

- Updating a core identity if attributes such as the person's name changes.
- Renewing credentials, including foundational documents. Most credentials need to be renewed or refreshed.
- Re-verifying is normally a part of maintaining a person's identity. Typically this is done when credentials are renewed, but sometimes when there is a very important transaction or some question or doubt about identity has come up.

"Restoration" of a person's identity arises in circumstances where a person's credentials have been lost or "stolen" or misappropriated. This is a process where a person gets a new credential so they can access their goods, services or assets etc. The old credential should be cancelled so that it cannot continue to be used. If the credentials which are stolen or lost are fundamental credentials, the process of restoration can be very involved and time consuming. It may mean having to re-establish a person's core identity.

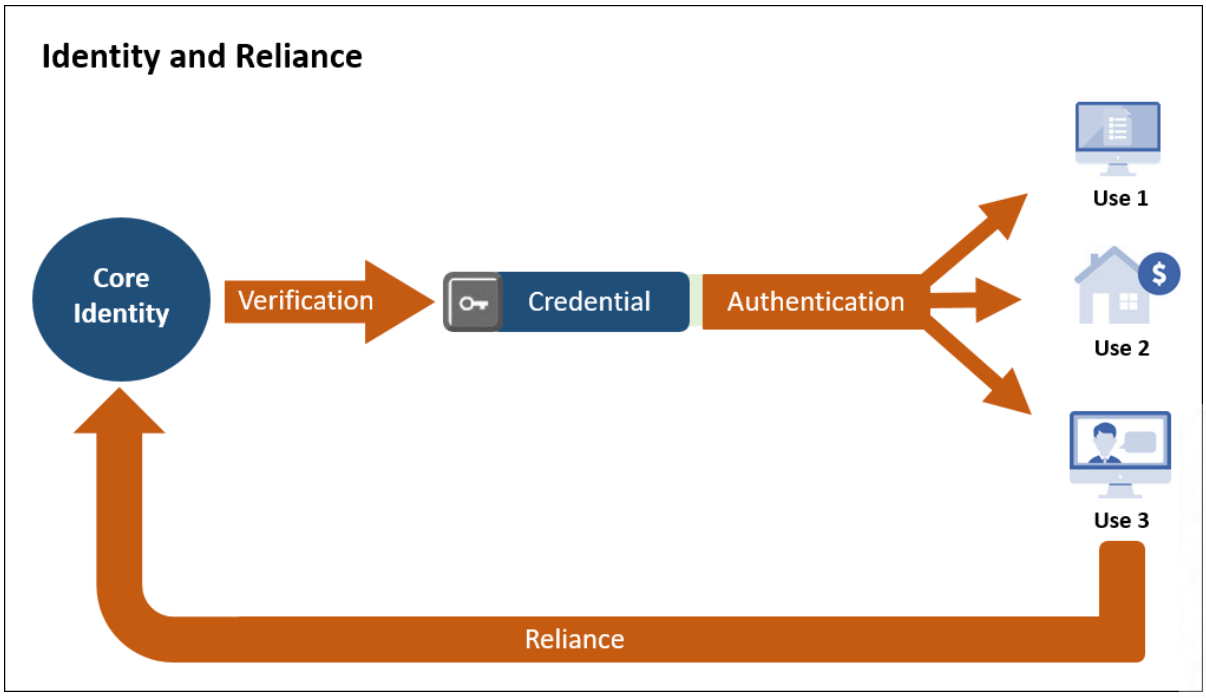
"Retirement" of identity is a process of cancelling an individual's credentials. Typically, this is because the person has died. But it may also be part of the process of restoring a person's identity.

4.2 Reliance and confirmation

There is an important aspect of a "system" of identity that needs to be understood. When a bank authenticates Roger Wilkins' identity using his bank credential, or,

looked at another way, when Roger Wilkins uses the credential provided by the bank to successfully withdraw money, all of that is some confirmation of the reliability of the credential. The strength of the confirmation depends on the frequency of use of the credential and the probability that any problem will be discovered. For example, banks now have a process of informing a person that their account or their credit is being accessed, giving them the opportunity to intervene. That is a way of preventing or discovering a problem.

Setting up systems that confirm or disconfirm reliability is very important for the reliability of an identity system. The successful and unproblematic use of the credential confirms, to some extent, not only the credential, but also the document and proofs that were relied on to issue the credential.



"Confirmation" is the other side of the coin of "reliance". "Reliance" is the critical relation in the system. A system of identity is a system of "reliance". In verifying Roger Wilkins' identity the bank relies on the credentials created by those agencies that proofed Roger Wilkins' core identity. The agencies might include the

Department of Foreign Affairs and Trade (DFAT), the Department of Home Affairs (Home Affairs), Driver Licence Agencies (DLAs).

Whether it makes sense to rely on a credential will depend on two things:

1. The reliability of the credential i.e. the probability that a person using the credential is not the person they claim to be.
2. The importance or significance of the consequences if the credential turns out to be wrong.

In the parlance of decision theory (1) is the "probability function" and (2) is the "utility function".

In designing a system of identity, it is mainly factor (1) probability of being wrong that we can influence. Factor (2), the consequences of being wrong, will vary from situation to situation and will be subjective to some extent.

The key thing is that companies and government agencies need to make a deliberate decision and set clear policy about whether, when and how they should rely on customers or citizens credentials. That requires a proper risk assessment.

A coffee shop selling customers coffee and cake is not going to worry much about authentication of a customer's identity. But a bank giving customers credit or a government department paying people pensions is going to be much more concerned to establish a person's identity.

A system of identity, then, is a system of reliance and the strength of a system of identity, mainly has to do with the reliability of the credentials for proving an identity. Reliability is a function of the probability that a credential works and the likelihood that if there were a problem, that we would discover the problem. If the probability of a credential working is very high, and the likelihood of discovering a problem if there is a problem is also very high, then the credential has high reliability.

4.3 Why and how we want to maximise reliance?

To the extent reliance is maximised in a system, the number and complexity of credentials and methods of proof should be reduced to a minimum.

This should have a significant impact on the "transaction costs" in economic and social transactions.

However, it is important to understand that there are some costs that will need to increase:

- First, proofing a person's identity, establishing a person's core identity needs to be carried out to a very rigorous standard and maintained.
- Second, the discovery of problems and the flow of information about the problems in the system will not be costless.
- Third, managing or coordinating the system so that standards are observed and problems discovered and sorted out is not without cost.
- Fourth, the question of liability or "warranting" or "guaranteeing" reliability, will involve at least contingent costs (if a credential or method of proof is not warranted or guaranteed, then the cost of dealing with that risk will fall to the relying party, or be passed through to the customer).

A few other observations about "reliance". First, we can think of a "chain of reliance" as a sequence. Where X is wanting to verify Roger Wilkins' identity, X could rely on a credential that Y has given Roger Wilkins, and Y in turn may have relied on a credential that Z has given Roger Wilkins. The chain could be a long chain of reliance. Our view is that it is better to have shorter "chains of reliance", rather than longer. The reason is fairly obvious: in a longer chain of reliance there is more opportunity for things to go wrong.

Second, there are rough sectors or "communities of interest" such as the "financial sector" or the "government sector" or the "utilities sector". What tends to distinguish these sectors is that citizens or consumers want to be able to move costlessly and "seamlessly" across the sector. The idea of open banking or "joined up government" or shopping around for the best energy or telecommunications deal, are examples of that. Having a single credential or method of proof for identity across these sectors would significantly enhance competition and efficient service. In this instance reliance would be "horizontal" so to speak, rather than simply "vertical". This type of "horizontal" reliance may need to be "facilitated" or mandated by government in the interest of competition.

Third, the advent of digital ID's potentially makes the processes of verification and authentication of identity both much easier and much harder. It makes it much easier to have a single identity for all purposes and to identify interference and misuse and deal with issues of restoration of identity. It makes it much harder because the whole issue of cyber security needs to be properly dealt with.

We do not think it is sensible to prescribe in detail how a system of identity will or should operate.

We do think it is important to say how the fundamentals should be put in place. It is like providing a piece of critical infrastructure. People who provide and maintain roads or railway lines do not get involved in deciding about what roads or railways should be used for. That is a matter for users to decide. Providers of transport infrastructure might be concerned about rules of the road, questions of maintenance, the weight of vehicles etc. but not the private purpose for using the infrastructure.

If we think of a system of identity as "critical infrastructure" it is more like the standardisation of weights and measures, or providing a currency system than transport infrastructure. Napoleon introduced a standard meter rod in Paris as a

reference point for all measurement. This standard meter does not measure anything, but it "governs" the entire system of measurements in meters. It enabled Napoleon to reform an ad hoc and confused system of measurement based on lots of different local standards and variations. It was not a system that had anything to say about what to measure or why things should be measured.

Centralised systems of issuing and controlling currency displaced a "balkanised" system or systems based on promissory notes or credit / "I.O.U's". The value of currency depended on how trustworthy the issuers of the notes were – the "substance" and the "honesty" of the person or organisation. Under these circumstances the value or reliability of the notes was variable and difficult to know or prove. Accordingly, its fungibility, stability and portability was limited. Systems of state based currencies attempt to address these issues by providing (mostly) greater guarantees of substance and honesty, and hence greater fungibility and stability.

We think a system of identity should be similar to the cases of measurement and currency. A system of identity should provide citizens and residents with a reliable way of proving who they are. When and why people choose to use their proof of identity is a matter largely for them and businesses and organisations who want to supply them goods and services.

It is interesting to consider the alternative. In the cases of measurement or currency, we know that there are different systems in the world, and we know that involves high transaction costs and inconvenience. We know that before the emergence of standardisation there was little confidence or trust in the value of currency; it relied on personal relationships and "social capital". We know that measurement was a risky business that continually needed to be checked and supervised and different standards converted.

With identity, we are currently living in a world that resembles the "pre modern" world of currency and measurement.

As we will see, in Australia a person's proof of identity is not very strong. There are lots of different credentials and proofs of identity. The reliability of those proofs is variable. The costs of managing identity are very high, and are borne to a significant degree by individual citizens and consumers.

5. What principles or criteria should govern the design of a system of identity?

PRINCIPLE 1: Right and Obligation to an Identity

All citizens have both a right and an obligation to have a means of proving their identity.

PRINCIPLE 2: Utility

It should be as easy and inexpensive as possible for people to get, use and maintain a method(s) of proving their identity.

PRINCIPLE 3: Reliability

The methods of proof available should be as reliable as possible, commensurate with the level of risk involved.

PRINCIPLE 4: Privacy and Security

The amount of personal data collected and used should be as little as possible and should be stored securely.

Except in clearly defined circumstances where it is necessary to access or use the data in the public interest, the consent of the person concerned to the use of the data should be required.

PRINCIPLE 5: Strong Verification

A person's identity should be verified to a high standard.

PRINCIPLE 6: Maintenance and Restoration

Any agency or organisation that verifies a person's identity should take all reasonable steps to maintain and restore (if necessary) the methods of proof or credential it gives the person.

PRINCIPLE 7: Reliance

Agencies, businesses and organisations should only authenticate a person's identity when it is necessary to do so, and as far as possible, should rely on existing credentials.

PRINCIPLE 8: Interoperability and Portability

A verified identity and the credential issued as a consequence, should conform to standards that enable it to be utilised and accepted as widely as possible both internationally and domestically.

PRINCIPLE 9: Resilience

Problems and weaknesses need to be anticipated, discovered, notified and rectified as quickly as possible with minimal disruption.

PRINCIPLE 10: Responsibilities

Obligations and responsibilities within the system need to be clearly articulated, understood and complied with.

These are general principles drawn from a number of different sources and considerations. We have considered ideas expressed in expert reports, submissions and roundtable discussions.

There are a few considerations that are going to be important to our thinking which may not amount to "principles".

One is that we should avoid "over engineering" or "over systematising" things. Any system will have interdependencies. Clearly, strong identity verification is something we think is critical and that other parties should rely on. This is a critical interdependency, but this need not involve anything elaborate or high maintenance or prescriptive, other than requiring a high and reliable standard of verification.

We believe that the Australian "system" is moving in this direction anyway, albeit imperfectly and slowly.

And that is the second consideration; we will try as far as possible to use existing institutions and existing processes and initiatives. It is not desirable or practical to start with a blank slate.

6 What are the challenges with the current system

The current "system" of identity in Australia is essentially a legacy system attempting to come to terms with the emergence of the internet and the information economy and with impacts of 'globalisation' on society and the economy. That includes the increasing "commodification" of personal information.

6.1 No one is responsible

Australia's identity 'system' has grown in an ad hoc manner without much policy guidance or direction from governments. It has been frequently observed by stakeholders engaged by the Review that identity management is disconnected and fractured across government. This reflects the fact that Australian governments, in the time since the failure of the Australia Card, have avoided pursuing a national identity policy explicitly defining the need for a single identity credential as a public good.

In the absence of such a scheme, the alternative is to depend upon a range of existing documents that contain identity information; however, these documents are primarily designed to demonstrate eligibility for different benefits and entitlements and are managed accordingly.

This is further reinforced by the fact that identity is an enabling element of service delivery – not its core purpose. With responsibility for identity matters often delegated to an agency level, policies are developed with an enterprise view and credentials are issued and managed to suit a business function's specific requirements. The risk tolerances of identity issuance, proofing and management in such a context is typically shaped within that specific service agency's perspective and principally for their benefit. It is often unclear how a whole of government view is communicated and coordinated let alone a national one is achieved.

In fact, it is impossible to identify who it is in government that is responsible for "identity". Policy and practice in government is more often than not "balkanised" among different departments and agencies, and among the Commonwealth, States and Territories.

For individuals it is often even more difficult to understand who they should be dealing with for questions regarding identity, particularly where the verification of their identity may involve multiple agencies at both the Commonwealth and State and Territory levels.

6.2 There is no real "national" approach to identity

There is no national policy for "identity" in its own right, nor is there any authority or department in Australia that has overall responsibility for identity, or even policy and coordination of practice around identity.

While the National Identity Security Strategy (NISS) provides the basis for a policy framework and collaborative action, s. 37(2)(c)

Responsibility is split between the Commonwealth and the States and Territories. Historically, the States have taken a "State" view of identity and the Commonwealth, a "Commonwealth" view of identity. s. 37(2)(c)

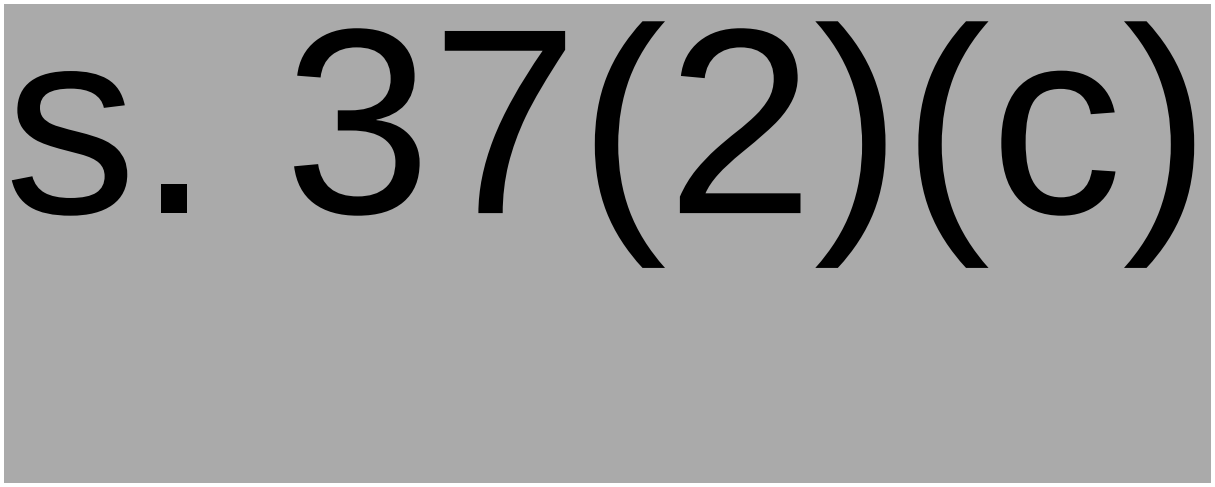
The movement toward a "national" approach to driver licences, births, deaths and marriages and associated data is very slow and gradual. It has certainly failed to keep pace with mobility and social and economic change in Australia.

The drive to online service delivery has also seen the development of multiple digital ID schemes across the jurisdictions, each promising a "trusted identity" that can be accepted for multiple services. The national remit or interoperability of any of these schemes remains unclear, posing the risk that the future digital platforms for identity may yet strike a very real 'rail gauge' problem.

Of greater concern is that many of these schemes are in essence registration schemes for online service-access credentials which are reliant upon existing document-based arrangements. However, these digital ID schemes are not addressing the weaknesses of the system of physical documents which they aim to replace. This risks simply migrating known failings into a cyber-environment of amplified exposures and escalating impacts, and represents a failure to connect digital ID efforts into a broader national identity policy discussion and governance framework.

6.3 A "system" still based on documents

The "system" of identity in Australia is still largely based on documents (both their physical presentation and related electronic record), including: birth certificates, passports, driver licences, Medicare cards, utility bills and citizenship certificates, all of which have known vulnerabilities.



s. 37(2)(c)

6.4 The purpose of key "identity" documents is not identity

Some of the key identity documents—driver licences, passports, Medicare cards, even credit cards and utility bills—are not primarily documents designed for that purpose. They have come to be used as identity documents, but historically that has been a by-product of their primary purpose. For example, s. 37(2)(c)

There have, however, been a number of recent agreements and initiatives that should assist in improving the situation:

- The creation of the DVS and the FVS.
- The issuing of the National Identity Proofing Guidelines (the NIPGs).
- The agreement to adopt a uniform national approach to issuing and managing driver licences.

6.5 There is no logical framework

There is really no adequate identity "framework" that is both nationally endorsed and provides general guidance to citizens, business and government agencies about how the verification and authentication of identity should work; how those processes should relate to issues of data protection, privacy and the emergence and proliferation of digital ID's; and there is virtually no guidance about the maintenance and restoration of identity.

While the NISS has established a framework for national policy around identity proofing many elements of identity management have yet to be articulated particularly around authentication, maintenance, the recovery and restoration of

identities and their eventual retirement. This represents a significant gap in policy coverage, which skews focus on establishing an identity but not its ongoing upkeep and protection.

While there are technical and data services available which could support a more cohesive approach to protecting and managing the identity "life-cycle", these more often than not remain latent or under-used capabilities for want of a clear policy requirement.

6.6 There are no standards

There are no nationally endorsed standards for identity management which apply broadly across public and private sectors. In fact there are multiple identity standards which apply in various contexts including regulatory requirements for the banking and financial services or telecommunications sectors for example or as part of jurisdiction based digital services strategies. The NIPGs, developed by Australian governments under Council of Australian Government's National Identity Security Strategy, are well regarded and have had considerable influence across commonwealth, State and Territory agencies. However their application is not assessed and we do not yet know how well they have been implemented or, indeed, how effective they are. Furthermore, the NIPGs are not mandatory, even within government; and while these are the most commonly accepted reference point for many agencies they do not amount to an Australian standard.

There are agencies which have adopted the NIPGs as a default requirement but note that the ambiguity or high-level nature of the Guideline's language limits the efficacy of their implementation as a standard.

6.7 The foundation is weak

The establishment or creation of an identity, through the commencement of identity record, is the foundation of identity in Australia and remains a fundamental weakness. A birth certificate is, for most Australians, the commencement of identity, and it still plays a critical role in identity. Passports and driver licences for example, are issued largely on the basis of birth certificates. Birth certificates, however, are not biometrically based and are relatively easy to misuse.

For those that come to Australia, their commencement of identity credential is initially a visa. The level of quality and reliability in visa systems are dependent in large part on foreign identity documents, commonly a passport, presented by the individual and the biometric data that may or may not be captured through visa processes. Documentation for people who come to Australia from overseas is even more problematic, depending on the documentation they have and the country that issued them.

Having weak commencement of identity document issuance and management process has a flow-on effect on the overall integrity of the identity system. These inherent weaknesses are further perpetuated across the system as the identity is reused as the basis for other identity proofing processes.

The fundamental problem with the birth certificate and Medicare card is not in the way they are issued, but that there is no secure and reliable biometric linkage to the person and there are no subsequent steps to effectively biometrically “bind” the registration or the document to the individual. Consequently it is relatively easy for someone to misappropriate these documents for the purposes of obtaining a driver licence or passport.

Adequate binding is also an issue with visas. Currently biometrics are only captured for about 6-7% of visas issued by Home Affairs. Given that the visa is a commencement of identity document for foreign born individuals in Australia and that overseas born individuals represent an increasing cohort of the Australian

population, this represents a significant shortfall and missed opportunity to better anchor the identity of a growing part of the community.

s. 37(2)(c) [redacted]

6.8 The "100 Point check" does not make sense

The "100 Point check" is used as a default standard for issuing identity credentials, or high level verification of identity. Originally introduced in the wake of the failure to create an "Australia Card" in the late 1980s, the "100 Point check" has become a common reference for identity processes operating within many agencies and private sector organisations.

It is not a very rigorous standard as it can be satisfied with multiple low integrity and easy to forge documents such as library cards, utility bills, and concession or Medicare cards.

Central to the weakness of the current "100 Point check" is the failure to require a biometric foundation for a person's identity and the failure to check or authenticate that biometric identity for critical transactions subsequently.

And with no clear biometric matching requirement, someone intent on creating a fake identity would have little difficulty in doing so. In any event, the "100 Point

check" as it currently stands and operates resembles nothing so much as the old alchemists' dream of producing gold from lead.

6.9 Some Australians do not have identities

"Vulnerable people" include those people who do not have the required documents to establish or verify their identity. It also includes people who, for reasons of remoteness or reasons of disability, are not able to either establish their identity or use an identity document or method of proof to do things.

With an aging population there is an increasing number of people who will not be able to do things themselves. These people have difficulty accessing goods and services and government assistance. The increasing use of digital IDs and online services is tending to exacerbate this problem in some cases, and help solve it in others.

DHS pays around 700,000 people under alternate identity arrangements. Many of these individuals are unable to confirm their identity; however, some have not been asked to confirm their identity due to existing business processes which exempt them from the requirement to provide proof. This represents 20% of potential Centrelink clients who potentially are not able to prove their identity.

Under the current system, in order to issue a Customer Reference Number (CRN) and access government assistance, DHS has to carry out an investigation into the persons' background and history and "create" an identity for the person.

People not able to support themselves rely on documents such as authorisations and powers of attorney to appoint person(s) or an organisation to manage their affairs. This effectively means that two identities plus the link or authorisation need to be authenticated.

6.10 "Bootstrapping" is a critical weakness

s. 37(2)(c)

[redacted]

6.11 Biometric identity documents are of variable quality

Australians have some biometrically based identity documents. Passports and driver licences, for example. The emergence of biometrics as a basis for identity, is probably as significant as the emergence of the internet for transforming our 'system' of identity. The capability to verify and authenticate identity using biometrics has enormous potential to make the system of identity more reliable, more convenient, and a lot less costly and intrusive.

Currently, however, the issuance of biometric identity documents such as passports or driver licences or ImmiCards is of varying quality.

Passports are likely to be the most reliable document based on a biometric. The APO, for example, does a one-to-many check before issuing a passport to ensure that there is no duplicate passport under a different name.

This is not done for all State and Territory driver licences; and not all States and Territories even issue a biometrically based licence at present (NT and ACT). Where a

biometric is used, the International Organisation for Standardisation (ISO) and/or International Electronic Commission (IEC) standards could vary.

Appendix 4 provides more detail.

The quality of biometric data collected is also an issue with visas issued by Home Affairs. For most visa processes the collection of a biometric is limited within Australia with most biometrics being captured offshore through third party arrangements. This has led to a wide variability in both the quality and integrity of the images that have been collected.

6.12 People have an equivocal attitude to identity, data sharing and biometrics

People's attitudes towards the use of biometrics seems to be equivocal. They seem to appreciate that it can make their dealings and transactions much more secure and much more convenient. But they are worried about whether their biometric can be "stolen" or "compromised" and what happens then. They are also worried about whether biometric data could be used by governments or businesses for other purposes.

Response to the OAIC's Australian Community Attitudes to Privacy Survey in 2017 suggests that the community's comfort with the use of biometric information appears to be growing. But there is still some apprehension in the community about biometrics usage depending on the organisation or business transaction being performed (day-to-day banking, air travel).

An international survey undertaken by IBM of consumer attitudes toward identity and authentication also suggests a possible shift in community attitudes. The IBM study[2] was conducted across the United States, Europe, Australia, India and

[2] Future of Identity Security Study (Consumer Perspectives on Authentication: Moving beyond the password, 2018)

Singapore. The survey reported that 67% of respondents are comfortable using biometric authentication today and 87% of respondents would consider using different types of biometric authentication in the future.

6.13 There is no systematic process for resolving identity

By "identity resolution" we mean a process for investigating and figuring out a person's true identity where there appear to be multiple identities or no identity. The APO, for example, will sometimes need to do this if a person applies for a passport, but a one-to-many check indicates that a person has a passport under different names. DHS deals with people who sometimes do not have any of the standard documents relied upon to establish an identity. DHS therefore needs to "establish" the person's identity to assess eligibility for benefits.

In Australia, this process of identity resolution is only carried out by some agencies and there has been no real attempt to establish a "best practice" methodology or standards across the system.

The NIPGs require that problematic cases of identity be noted and listed. But there is no attempt to explain what identity document issuers might do by way of identity resolution.

Similarly with the renewal of identity documents there is an opportunity to "refresh" the verification of identity. But what that should entail is not clearly spelled out. It is likely that "renewal" is viewed mainly as a revenue opportunity.

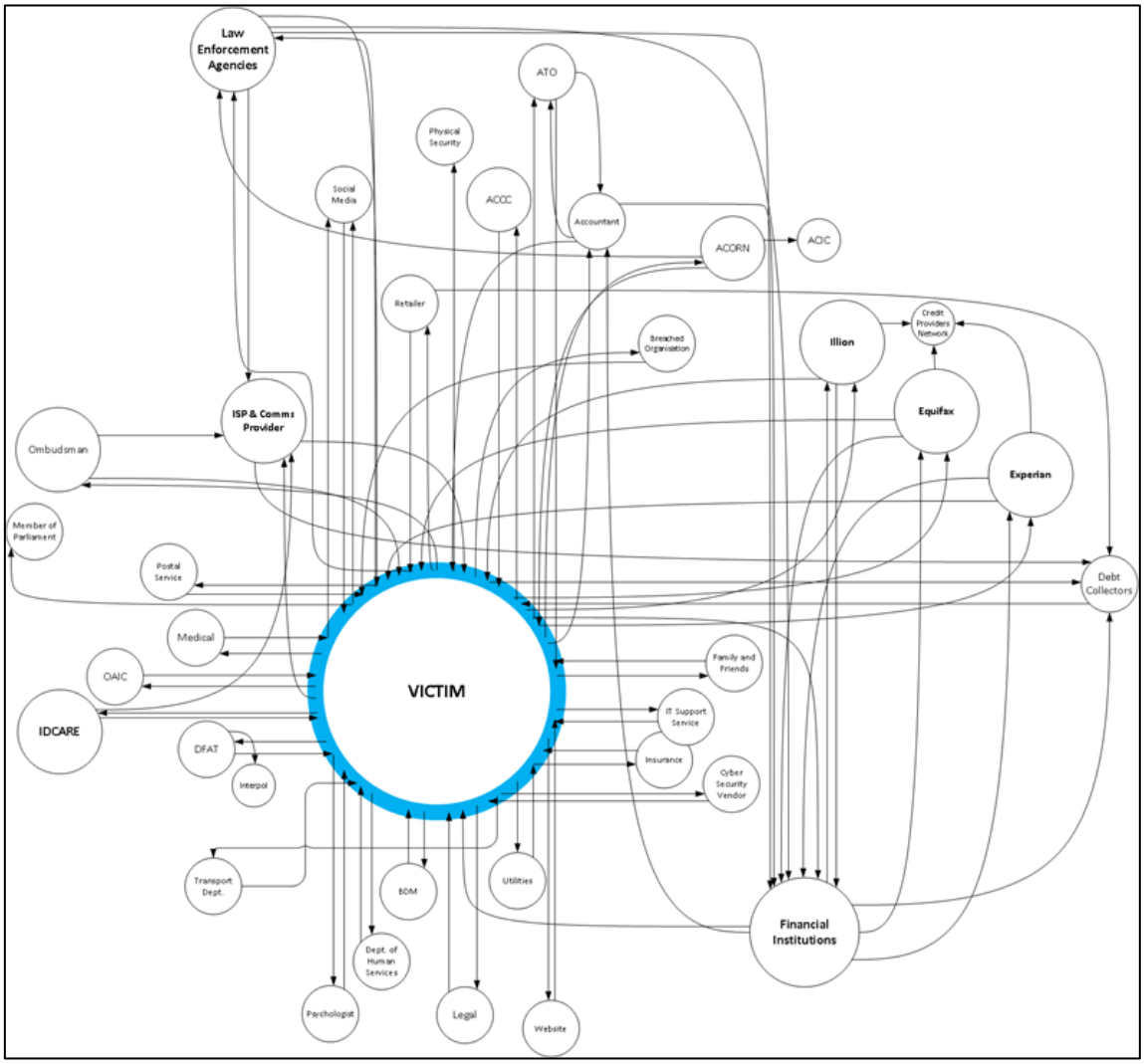
6.14 There is no system for the restoration of an identity that has been "lost" or "stolen"

The system is largely incapable of communicating in a timely manner information about lost and stolen identity credentials that reduces the risk of identity misuse amongst relying parties. The Review has received input from various identity

credential issuers that reveals that in any given year more than half a million credentials are reported lost or stolen. Despite this, and the nature of the system's reliance, little to no sharing of this risk occurs unless initiated by the victim of identity "theft" or reserved for limited subsets of industry that communicate amongst themselves.

The system is almost entirely dependent on each individual victim to contact multiple government and private sector organisations. As each organisation has unique processes the victim of crime is required to navigate multiple processes with the duplication ultimately adding to the harm and cost. On average an Australian will spend around 23 non-consecutive hours responding with many organisations (see below identity "theft" response network, Wyre, Lacey & Allan forthcoming). The Review observed significant deficiencies in response standards, formal reporting channels of Government, and meaningful protection measures for consumers. Overall the response system is either non-existent or performing poorly from a citizen's perspective.

The Social Network for an Identity "theft" Response System



Despite the emphasis on citizens, any subsequent identity misuse or loss that is based on the reliance of the stolen or lost credentials is typically a liability carried by the relying party. In other words, the citizen appears to be doing the heavy lifting of response, oblivious to the fact that they are actually doing all of this to prevent future losses to government and business.

6.15 There is no systematic approach to the maintenance or the retirement of identity

Most key identity documents are issued for a term and then need to be renewed. Passports and driver licences would be the key examples. The same is true of identity documents such as credit card and student cards.

However there appears to be limited thought given to the processes and protocols around the renewal of identity documents. It is a key opportunity to re-verify identity and should be treated as such.

Retirement of identity is effectively the death of the person. It would normally be the task of the executor or personal representative to ensure that the person's death is notified to issuers of identity documents, custodians of assets, debtors or creditors.

There is now a Fact of Death file managed by the State and Territory RBDMs. A person's death is noted in the RBDM registry of the jurisdiction where the person's death occurred. However, there is no uniform process ensuring that this is in fact noted or linked to the person's home register i.e. the RBDM registry of the jurisdiction where the person's birth is recorded, i.e. birth certificate was first issued.

Deaths occurring outside Australia are recorded where these events are notified to the relevant High Commission, Consulate or Embassy. These details are then passed on by DFAT to the ACT RBDM which in turn passes these details onto the QLD RBDM registry which compiles the Fact of Death file. There are however no fixed protocols for the reporting of Australian deaths overseas and the collection of this type of information is neither consistent nor timely – particularly to issuers of key identity documents.

6.16 Australia's identity system is duplicative and intrusive

Because of the weakness of identity credentials most businesses and even government departments do not rely only on these credentials when they are authenticating or

verifying the identity of their customers. They tend to rely more on their own systems of profiling and due diligence.

A bank, for example, or a government agency develops its own identity document and its own methods for assessing the consistency and coherence of transactions. In general terms, we call this “Know Your Customer” (KYC).

It is true that KYC is not merely a response to a weak identity system, and is not necessarily a negative. But the duplication of identity proofing as part of KYC is a problem.

From a citizen or customer perspective, it does mean that corporations or departments with whom they have ongoing dealings want to know much more about them and their transactions. Customers and citizens have to repeat things over and over to lots of different organisations.

It means that customers and citizens are having to manage an increasing number of identity documents, passwords, PINs etc.

We will consider the costs of this system shortly, but it is worth noting that the costs to business and government of KYC are significant. Not all of that is attributable to issues of identity verification and authentication but a lot of it could be. Fraud is one of the key things KYC is designed to prevent and we know that a significant percentage of fraud in both the public and private sectors is a function of compromising or stealing a person’s identity.

6.17 A key issue: citizen consent and control

Biometric information is “sensitive information” under Australia’s Privacy Act. It is information that can only be shared or used where the person clearly consents or the law clearly provides.

Notwithstanding that, many of the public submissions, discussions with people and organisations at sector workshops have expressed concern that changes to the identity system should not undermine this principle.

If anything, citizen consent and control need to be enhanced.

A complicating factor is this: increasingly the "capture", storage and use of personal and sensitive information of Australians is not necessarily occurring in Australia, and may be beyond the effective jurisdiction and control of Australian law and authorities.

It is a function of the global mobility of people, goods and capital.

Many commentators have described the "commodification" of identity information. There have been recent prominent cases involved Cambridge Analytica and Facebook which illustrate the process of harvesting bulk information about individuals.

Business and corporations are likely to be required in the future, either as a matter of "branding" or a matter of law, to put in place much more stringent practices to protect peoples' data and to disclose their policies and practices clearly. This would be similar to what the Europeans have already required under the General Data Protection Regulation.

There is an evident need to provide the public with better information and education about best practice on prevention and self-protection in relation to "theft" of identity data and information.

There is also an "industry" emerging around new online products and technologies designed to allow people to secure and control their information. For example the use of digital wallets or forms of encryptions or block chain.

Whether and how government should intervene in this space is a key issue.

6.18 The system of identity in Australia is relatively insecure and unreliable

Our modelling shows that overall Australia's system of identity is not very secure or reliable. It is roughly comparable to other Anglo-Saxon systems such as New Zealand and Canada. It is much less reliable than Israel's system which, like most of the continental European systems has a single national credential scheme as the basis of the system (see Appendix 1).

Data on the incidence of identity "theft" and identity compromise show that a quarter of Australians will experience identity "theft" or compromise.

Data from IDCARE in February 2019 indicates that the top five most commonly targeted identity credential information are:

- Mobile phone account information
- Driver licence details
- Bank account information
- Passport information
- Medicare details

At the time of reporting incidents to IDCARE, 58.6% of community members had experienced both the "theft"/compromise of their identity credential and personal information as well as criminal misuse (i.e. other criminal offending based on the misuse of the compromised identity credential and personal information). Our view is that a lot of the problem is bound up with the weak foundations and weak establishment of identity in the Australian system.

Many of the negative effects experienced by citizens, consumers and taxpayers are a result, directly or indirectly, of this problematic and weak establishment of identity.

The introduction of the DVS appears to have had a positive effect in countering the use of "fake" or "fictitious" identities. However, we are seeing an increase in the range of criminal activity that involves the '"theft"' or "appropriation" or "compromise" of genuine identity documents.

This has a direct effect on citizens and consumers.

The results from Project Birrie, a multi-agency data-matching initiative led by the AFP-hosted Fraud and Anti-Corruption Centre confirm that criminals use fraudulent identities to avoid detection by authorities. The purpose of the Project was to measure the nature and extent of criminal offences enabled by the fraudulent identities manufactured by one organised crime syndicate. It involved the examination of 1,710 fraudulent identity items seized from the organised criminal syndicate in New South Wales. The findings which are available at Appendix 2 highlight the key role that fraudulent identities can play in enabling a raft of other more serious offences, such as money laundering, drug trafficking and large financial frauds.

6.19 Law enforcement is relatively ineffective in combatting identity crime

Investigating and prosecuting identity crimes are problematic for law enforcement due to a range of factors. Jurisdictional differences place considerable pressure on law enforcement to determine the offender's geographic location, which can be within an offshore policing jurisdiction and subsequent responsible policing jurisdiction.

Variability in law enforcement approaches toward reporting and tracking of identity crimes also impacts on the successful investigation and prosecution of these perpetrators. For example, New South Wales Police accept reports of online identity crimes over the counter; whereas other States and Territories do not, preferring to exclusively refer community members to Australian Cybercrime Online Reporting Network (ACORN).

Where complaints do result in a presentation of the victim to a police station, the relatively high-volume low-value nature of identity crime offending contributes to prioritisation challenges for law enforcement. This traditional law enforcement approach has limited utility in the context of identity crimes and is likely to cause additional harm to the victim.

The time taken to investigate versus the enduring risk of identity misuse also creates problems for both complainants and law enforcement given the dynamic nature of identity crimes. It is common for victims to have ongoing and repeated engagement with identity thieves even after they have made initial reports to law enforcement and law enforcement simply does not have a scalable capacity to intervene in most of these matters. The recently published Australian Institute of Criminology evaluation of ACORN reaffirms that "very few finalised investigations resulted in an offender being apprehended" [3]. This creates further problems managing the expectations of the community in relation to law enforcement's ability to respond to such crimes. For example, in terms of online scams only fifteen per cent of complainants received formal notification from law enforcement that their report was received and that their matter was investigated, compared to less than one per cent who were notified of these actions *as well as* an offender being arrested[4]. Around 78% of respondents to the Australian Institute of Criminology's review of ACORN expected that their report would be investigated by law enforcement. This expectation is arguably further heightened for individuals where they continue to receive unwanted contact by the alleged offenders directly or where the victims experience future identity misuse (further criminal offending using the victim's identity).

Despite the relative ineffectiveness of law enforcement in addressing problems of identity "theft", it is still necessary for victims of identity crime to obtain a Police Report Number in order to prove they are a bona fide victim.

6.20 The Australian System is costly and costs are likely to increase

A major cost for citizens and consumers is the cost of managing a proliferating number of identity documents. This includes enrolling to get the identity document;

[3] Morgan, A., Dowling, C., Brown, R., Mann, M., Voce, I., & Smith, M. (2016) *Evaluation of the Australian Cybercrime Online Reporting Network*, Canberra: Australian Institute of Criminology

[4] Ibid.

authenticating its use; and very often spending an inordinate amount of time, effort and sometimes money to restore a lost or stolen identity document.

Identity documents are designed primarily to protect the interests of the agency or company from liability of various kinds. Verification and authentication requirements are becoming more rigorous and onerous. For consumers and citizens this is both good and bad.

Transactions are becoming more complex. For citizens and consumers to carry out relatively simple activities they may have to use several IDs – to set up a computer, change a utility provider, organise a holiday etc.

The Australian Institute of Criminology study found 25% of Australians have had their identity stolen or compromised[5]. Even though in many cases the loss being avoided would likely be that of the relying party of the identity document, it is the consumer who is left to investigate the loss and "restore" their identity. The average time it takes to deal with the "fall out" of a loss or "theft" of identity and restoration is over 23 hours. On top of that there are various behaviour impacts and costs, including anxiety, frustration and overall trust in government and industry.

In 2017 the black economy was estimated to be as large as 3% of gross domestic product GDP (roughly $50 billion) which includes identity fraud and phoenix activity.[6]

In 2012, it was reported that Australians lost an estimated $1.4 billion through personal fraud incidents.[7] The problem continues to grow and in 2016 it was reported that the estimated direct and indirect costs of identity crime in Australia was $3 billion[8].

[5] Identity Crime and Misuse in Australia 2017, Australian Institute of Criminology

[6] Black Economy Taskforce, Final Report - October 2017

[7] Source Australian Bureau of Statistics (ABS) 2012, Personal Fraud 2010-2011

[8] Source Australian Bureau of Statistics (ABS) 2016, Personal Fraud 2014-2015

The impact of potential illegal phoenix activities was estimated to cost the tax payer between $1.8 billion to $3.5 billion. This represented approximately 0.11 per cent to 0.21 per cent of GDP in 2015-16.[9] Much of this activity is enabled through the use of fraudulent identities, or shortcomings in the processes for verifying the identity of person's taking out company directorships.

Australia Post has estimated that by addressing the gaps in the current identity system, up to $11 billion could be saved.[10]

Commonwealth entities invest heavily in systems to detect and minimise identity fraud. In 2017-18, fraud cost DHS $3.2 billion. Over a two-year period the Australian Taxation Office (ATO) saved $93.7 million by thwarting fraudulent attempts to obtain benefits or avoid tax liabilities through the misuse of identity.[11]

Advice from the ATO is that much of this fraud occurs through the use of multiple or fake identifiers. Advice from the DHS is that a great deal of this fraud could be avoided through a more robust system of identity. "Theft" or misuse of identity is a key enabler of organised crime. More of this "theft" or misuse of identity occurs online. Latest figures from IDCARE suggest that this could be as high as 69% in relation to the compromise of credentials, with almost all subsequent identity misuse events occurring online (i.e. 99.7% of reported misuse cases).

The cost incurred by major corporations such as banks, telcos and airlines in managing customer identities, conducting due diligence and authenticating various transactions is many millions of dollars. This is most often duplicated or replicated across the economy. These costs are eventually passed through into the costs of goods and services or reduced dividends or profits.

[9] PWC- The Economic Impacts of Potential Illegal Phoenix Activities, July 2018
[10] Australia Post, A frictionless future for identity management White Paper December 2016
[11] AIC Report, identity crime and misuse in Australia 2017

Governments spend many millions of dollars managing identity. This tends to be replicated across agencies or programs. There have been recent attempts to create "one-stop-shops" to break down boundaries between agencies and provide citizens with a "single portal", but no government has yet succeeded in offering citizens a truly portable credential. This has also proliferated an "arms race" as agencies attempt to develop a solution in isolation.

Perhaps even more significant is the opportunity cost in having a relatively weak and uncoordinated system of identity. A secure, reliable and portable ID would open up a large range of opportunities to reform the economy. A number of previous inquiries have noted how important a strong and portable identity is for economic reform.

The World Bank has published a number of reports that have case studies of how reforming the system of identity has improved social and economic outcomes. Estonia, for example, has one of the world's oldest and most advanced foundational ID systems. The system is underpinned by a national population register and a smart eID card. The estimated fiscal impact of Estonia's eID system has increased GDP by some 2% annually as a result of improving the efficiency of identity-related transactions and bringing 99% of services online[12].

Concrete examples in Australia would be "Open Banking" and efficiencies that could be generated if Australia had mutual recognition or portability of customer due diligence within the finance and banking sectors.

[12] World Bank Group, Public sector savings and revenue from identification systems: Opportunities and Constraints.

6.21 The internet and online transactions are making the question of identity ever more critical

Australians are increasingly accessing more and more online commerce, banking, government services, shopping, entertainment, social media, education, etc. This trend is expected to significantly increase as more online services become available.

Because online transactions are necessarily remote transactions, identity is becoming more important. Authentication is an integral part of every online transaction and relationship.

This has resulted in a proliferation of digital IDs or identity documents.

However, the internet is intrinsically insecure. We know that most identity "theft" is done through the use of the internet as part of cybercrime. There is an industry engaged in "retrofitting" the internet for security. The business of verifying and authenticating identity is a critical part of that.

Increasing the rigour and sophistication of verification and authentication online has also tended to make the process of obtaining, using and restoring identity documents more complex and difficult for citizens and consumers.

Much of cybercrime, including the compromise and "theft" of digital IDs cannot be combatted effectively using conventional law enforcement techniques. For one thing, attribution is often unprovable and mostly, perpetrators are beyond the jurisdiction of Australian law and law enforcement.

That places even greater weight on the importance of crime prevention; and the protection of identity and having a strong system of verification and authentication are a critical part of crime prevention in the internet age.

6.22 The internet is changing citizen's expectations about government

Citizens expect to be able to deal with governments online. Governments recognise that expectation and the opportunities this presents in providing interactions that are

simple and fast. There is now something like a “race” in our federal system to get to citizens with a digital ID. Almost all States and Territories and the Commonwealth are in the process of developing or rolling out digital IDs.

We do not want to get into detailed prescription about digital IDs in this report. But we do want to make a key number of observations.

Any digital ID still has to be soundly based i.e. there needs to be a strong process of verification and authentication. It is no different to a conventional ID or credential in that respect.

The use of any digital ID also needs to be subject to strong authentication in a range of cases. And that, too, is no different to a conventional credential.

Perhaps our key observation is that there is right now, the opportunity to ensure citizens have a single ID to deal with all governments and maybe business if they choose. Provided that is a “skinny identity” and soundly based, it should provide citizens with much greater convenience, reliability and security than a proliferation of identity documents.

We also find it difficult to understand how having more than one digital ID and no ongoing facility to do a biometric check would not open up possibilities of criminal misuse and duplicity.

Finally, with the current state of technological development, devices play a key role. The smart phone or the computer. In future this may not be the case, but right now having control of the device and or its number or address is a key aspect of a person’s identity. Email address and phone numbers are becoming key corroborating attributes linked to a person’s identity. We observe, however, that the process of linking these devices and numbers to the person securely is not currently done systematically or rigorously.

6.23 Failure of reliability and reliance: not being "economical" with identity

A key theme of our diagnosis about what is wrong with the Australian system has to do with the Principle of Reliance. This principle says roughly: businesses and governments should not proliferate identity documents but rather rely on soundly proofed credentials that already exist.

The problem is that for a range of reasons, there are few proofed credentials that are really reliable. Certainly, businesses use "100 Point Check", but then often proceed to put their own identity documents in place.

The result is that we end up with a proliferation of identity documents that cost consumers, businesses, and governments a lot of time, effort and money. We also end up with more personal information being asked for and provided much more often than it need be. This is what we mean by "not being economical with identity information".

Reliability is not the only reason why the principle of reliance does not work. There are some regulatory regimes that in fact prevent its operation. For example, the current requirements for financial institutions to undertake KYC for money laundering purposes does not permit a system of reliance or mutual recognition.

And then there is the related issue of liability. If X relies on Y's proofed credential and that turns out to be flawed, who is liable for the failure? There is no simple straightforward answer to that question. It will depend upon a range of factors:

- any agreement between X and Y
- any representations by Y
- any explicit reliance by X
- industry codes/best practice
- industry structures and arrangements.

7. Reforming the System

Citizens, consumers, businesses, organisations and government agencies want an easier, cheaper and more secure and reliable way for people to prove their identity.

Governments should provide that. It is not that the private sector cannot and will not do it. In fact private corporations already provide a variety of credentials that people use to identify themselves – banks, Facebook, PayPal. But all these credentials to some extent rely on basic documents or credentials provided by government.

There are good reasons for governments to provide "core identity credentials".

Governments are accountable to citizens in a way private sector corporations are not.

Governments do not have ulterior reasons or commercial agendas to pursue.

Governments also have a monopoly on the power to make laws and standards with universal application; and on the legitimate use of coercion.

Importantly, governments are already providing citizens with credentials that can be used to prove their identity. It is just that it is not being done in a very coordinated or efficient way.

Governments need to create sound foundations and a national framework for the establishment, management and protection of identity. That framework should enable citizens and businesses to prove their identity in an easy, secure and reliable way.

The development of a model to compare identity systems was commissioned as part of this review. KPMG and Home Affairs have worked on the model. It is not yet complete, but it does provide some comparative indicators. Those results are available at Appendix 1, and they tend to show that the reforms we advocate are

likely to have a substantial positive effect on integrity, and the ease and cost of using core credentials as a basis for identity verification.

The key components of a national framework for the management and protection of identity has the following four elements:

1. *Core credentials*

   Every Australian citizen or resident should have a "core credential" which is biometrically anchored, proofed to a high standard, and linked to a birth certificate or citizenship certificate or visa.

   This core credential should prove a person's "skinny identity"- name, date of birth, biometric.

   This "core credential" could be a passport, a driver licence, an ImmiCard or a Proof of Identity Card.

   These "core credentials" should be free.

2. *Reliance on core credentials*

   Where a business or government agency needs to verify a person's identity, it should rely on a person's core credential(s) using the Document Verification Service or the Face Verification Service. There would be no need to carry out "100 Point Checks".

3. *Identity Code*

   There should be an Identity Code (IC) that includes standards and rules that define rights, responsibilities and accountabilities for the collection, use, maintenance and management of identity information and core credentials.

4. *Office of Identity Protection and Management*

   There should be an Office of Identity Protection and Management that has overall responsibility for the "system of identity". It would have four main functions:

- Establishing and publicising the rules and standards that "govern" the system (IC).
- Ensuring these rules and standards are being complied with.
- Dealing with complaints and problems.
- Identifying and addressing emerging trends and challenges.

In an important sense, none of this requires radical change to what is already occurring. What it does require is higher standards of proofing and verification and better coordination. It also requires greater urgency about a range of initiatives that are "in the pipeline":

i. Completion of the FVS.
ii. Making the FVS available to the private sector.
iii. Completing the agreement to institute "one person, one licence", with the concomitant improvements in standards of proofing and collection of biometrics.
iv. Improving the exchange and integration of data between Registries of Births, Deaths and Marriages across Australia.
v. Improving the process for issuing visas and ImmiCards.
vi. Improving the process of "identity resolution", particularly for people who do not have much or any documentation.
vii. Completing the digital ID initiative.

1. Core credentials

"Every Australian citizen or resident should have a "core credential" which is biometrically anchored, proofed to a high standard, and linked to a birth certificate or citizenship certificate or visa[13].

[13] Facial biometrics have been selected as the most usable form of biometrics as they are less intrusive than others such as fingerprints and iris images. They are also simpler to collect, and are more socially and culturally acceptable.

This core credential should prove a person's "skinny identity"- name, date of birth, biometrics.

This "core credential" could be a passport, a driver licence, an ImmiCard or a Proof of Identity Card.

These "core credentials" should be free.

How does everyone get a core credential?

Most Australians have at least one "core credential", but not all do. "Proof of identity" documents are now more generally available and can be used by the people who have no need for a driver licence or passport. Typically, they are issued by DLAs and the APO.

"Proof of Identity" cards should be proofed to a high standard and offered widely to people free of charge. Anchoring a person's identity in a well-proofed biometric is a critical way of securing an identity and preventing identity "theft".

What is this higher standard of proofing?

This higher standard is essentially the standard currently being observed by the APO for issuing passports. The critical features of this standard are:

1) People have to turn up for an interview and will have to get their photographs taken in person.
2) The APO does a biometric check across the domain of passports already issued to ensure that there is no duplication (A one-to-many check)
3) Passports are periodically reviewed and renewed (at around 10 years)

Facial biometrics are a common feature in international standards including the International Organisation for Standardisation (ISO) and International Electro-technical Commission (IEC) frameworks (ISO/IEC 19794-5). Additionally, although reliant on the quality of images, facial recognition is considered a reliable form of biometric verification which is widely used internationally by governments and private industry. The accuracy and reliability of facial recognition algorithms continue to improve which is recognised in recent studies (NIST 8238) undertaken by the National Institute of Standards and Technology (United States Department of Commerce).

Other aspects of the procedures are obviously important as well, but 1 – 3 are critical for the reliability of facial biometric credentials.

All core credentials will need to be issued to this standard. Currently they are not, although a critical aspect of the intergovernmental agreement to establish the FVS entails applying this higher standard of proofing to the issuing of all driver licences across Australia.

It is important for citizens, businesses and organisation to understand the comparative reliability of various credentials. One simple and graphic way to do this is to classify credentials as “GOLD”. “SILVER” and “BRONZE”.

A “GOLD” credential like a passport would typically include the following:

1) A high standard of “capturing” the facial biometric, including a photograph taken in person.
2) A “one-to-many” check across the domain of credentials issued to eliminate the chance of duplication.
3) A check of the person’s other core credentials to ensure that there is a biometric match.
4) A periodic renewal of the credential (approximately every 10 years).

A “SILVER” credential would include a biometric, but the credential may be deficient because it does not include feature 2 above.

Currently some driver licence might be classified as GOLD and some as SILVER because some jurisdictions carry out a one-to-many check to eliminate duplication and some do not.

“BRONZE” credentials would be credentials that do not include a biometric. But these credentials will at least be based on appropriate documents and include a DVS check. There are some driver licences in this category.

This scheme of classification provides a guide to reliability, and importantly, an incentive for jurisdictions to improve the reliability of credentials.

Why link core credentials to commencement of identity records (birth certificates, citizenship certificates or visa for long term residence)?

For most Australians their "commencement of identity" in the Australian system is when they are born. Their birth must be registered with the relevant State or Territory Births, Deaths and Marriages Registry.

That fact of birth, and birth certificates, play a critical role in a person proving their identity and obtaining credentials, including core credentials, later in life. A birth certificate is part of the documentation required to get a passport or licence for example.

Birth certificates or birth registrations are not biometrically based. We know that they can be "stolen" and misused to create a fraudulent identity where someone pretends to be someone else.

We are not recommending capturing biometrics of babies or children. We are advised that facial biometrics, in any event, are not reliable for children until they are teenagers. What we recommend instead is that when the person does get a core credential of some sort with a biometric (passport or driver licence) that should be noted on their birth register and birth certificate; and vice versa, the registration together with the date of birth should be noted on the core credential.

Once that occurs it should not be possible for anyone else to pretend to be that person by using the birth certificate. The birth certificate from then on is effectively "bound" to a biometric.

We understand that various European jurisdictions, such as the Netherlands use this device of "retrofitting" a biometric credential. It does mean that there is a period of some years where the commencement of identity credential is not "biometrically bound", and that should be kept to a minimum.

We think the government(s) should consider offering all high school students a Proof of Identity card that is biometrically based for free.

For mature migrants coming to Australia either as a new citizen or on long term visas, we see no reason why the citizenship certificate or ImmiCard should not be a core credential with a biometric, or include the issue of a Proof of Identity card.

We understand that the Department of Home Affairs is already in the process of doing that for some clients.

Free Core credentials

"Core credentials" are the foundation of the system of identity. It is critical that all citizens and residents have access to these credentials. It is, in effect, a classic "public good".

If they were free and easy to obtain or actively offered, they are more likely to be taken up. In some cases where people want to drive or travel, there is effectively no choice. In other cases where the law or practice currently requires a "100 Point Check", there would certainly be good reason to get and use core credentials. Using a core credential would be easier and more secure, and constitute a "GOLD" standard of proof.

We think it creates an important incentive to offer core credentials free of charge. The money raised by selling core credentials is a relatively small amount of money in the scheme of things, and the benefits for society and the economy would be very significant.

In any event, we think the funding model for "identity" could be changed. Instead of charging citizens for the issue of credentials, governments could consider instead charging for the use of the credentials through FVS as well as the DVS.

Vulnerable People

There are some people who for a variety of reasons do not have documentation to "prove" identity and get a core credential.

Our consultations with States and Territories and DHS suggests there is a significant number of such people. They are also some of the most vulnerable members of the community. Very often they rely on support and services from government programs. In the absence of a

clear and easy way of establishing who they are, procedures can be complex and frustrating for them and the public servants involved.

The Department of Human Services and some States and Territories have an extensive program of what we call “identity resolution” i.e. a process of determining a person’s identity.

We think that where DHS “resolves a person’s identity”, DHS should also be able to issue the person with a credential that is biometrically based and can be readily used for access to services and programs across all jurisdictions. This would greatly improve efficiency and security as well as the person’s access to goods and services.

We also think that citizens who receive significant payments and benefits from governments should, as a matter of public policy, have an obligation to establish their identity.

Consolidating Processes

It should be possible for agencies that issue core credentials to cooperate so that a person only needs to turn up once to get their photograph taken in ideal conditions. The photograph could be used by different agencies as the basis for the person’s biometric core credential.

For example, a person could go to a Service NSW centre and have an interview for their passport, get the photograph taken for a passport and driver licence, and also have their identity verified for the purposes of a NSW Commonwealth digital ID.

There is a broad menu of options in this space to save time and money and make things much more convenient for citizens.

2. Reliance on core credentials

Where a business or government agency needs to verify a person's identity, it should rely on a person's core credential(s) using DVS or FVS. There should be no need to carry out "100 point checks".

Reliance on core credentials to verify a person's identity is at the heart of the system we are advocating. It means that the process of proofing a person's identity does not have to be repeated over and over again by different agencies and businesses.

Not all transactions will require a high level of identity verification or even any verification at all. Most transactions should not. The Identity Code (IC) will say that businesses and agencies should do a risk assessment to figure out what level of verification of identity is warranted. This should not be onerous. It is simply rational business practice that should be being done in any event.

In some situations the law will mandate the verification of identity, such as anti-money laundering laws. We suggest below a number of other areas where we think the verification of identity using core credentials and FVS should be mandated.

Mostly verification of identity using core credentials and FVS will require the consent of the person concerned. This is a basic feature of the way DVS and FVS should work. If someone does not consent then the alternative is to use a sound document-based proofing procedure supported by DVS checks. In a high risk scenario, that could also include, the need to obtain "attestations" of identity from "referees" who do have a "GOLD" standard credential.

3. The Identity Code

There should be an Identity Code (IC) that includes standards and rules that define rights, responsibilities and accountabilities for the collection, use, maintenance and management of identity information and core credentials.

It is easiest to picture the IC as a system of rules and standards that govern all aspects of the "identity system".

At 4.1) we set out the key processes that constitute an "identity system":

- Establish a person's identity or identity proofing
- Verification or "on-boarding"
- Authentication
- Maintenance and renewal
- Restoration of lost or "stolen" credentials
- Retirement or cancelling a credential.

The IC should set out the rights and obligations of the parties to each of these processes. But one very important aspect of IC is this: it should be built on a philosophy that when an organisation issues a credential it is responsible for the ongoing "health" and reliability of that credential. These processes are not isolated "episodes". Rather they should be thought as part of the "life cycle" of an identity.

At 5) we set out Principles that should govern the design of the system of identity. We envisage the IC as the systematic application of these Principles to each of the processes listed above.

The essence of the "identity system" we recommend is the sound proofing of "core credentials" (which is the first process listed above). These core credentials are then relied on and used by others to authenticate identity. It is likely that the code will have most to say about that process of identity proofing, and that will mainly concern these key public sector agencies involved in issuing, maintaining, restoring these critical core credentials (APO, DLAs, Home Affairs and DHS).

There are some matters in our recommendations that will obviously need to be embodied in the IC (citizen consent, higher standards for proofing, obligations to maintain and restore etc.). Mainly though we have taken the view that the task of constructing a comprehensive IC is beyond the scope of this report and is better worked out by those administrating the scheme in the new OIPM.

The question of sanctions and enforcement of the IC is important. Mostly we do not favour the use of fines and prosecutions. Public sector bodies are subject to ministerial direction and administrative sanctions. These can be invoked by the OIPM or even the Ombudsmen, or Auditors-General.

“Over legalising” the ICwill make it more prolix and bureaucratic than it needs to be, and it is not our objective to introduce a whole new area of “red tape”.

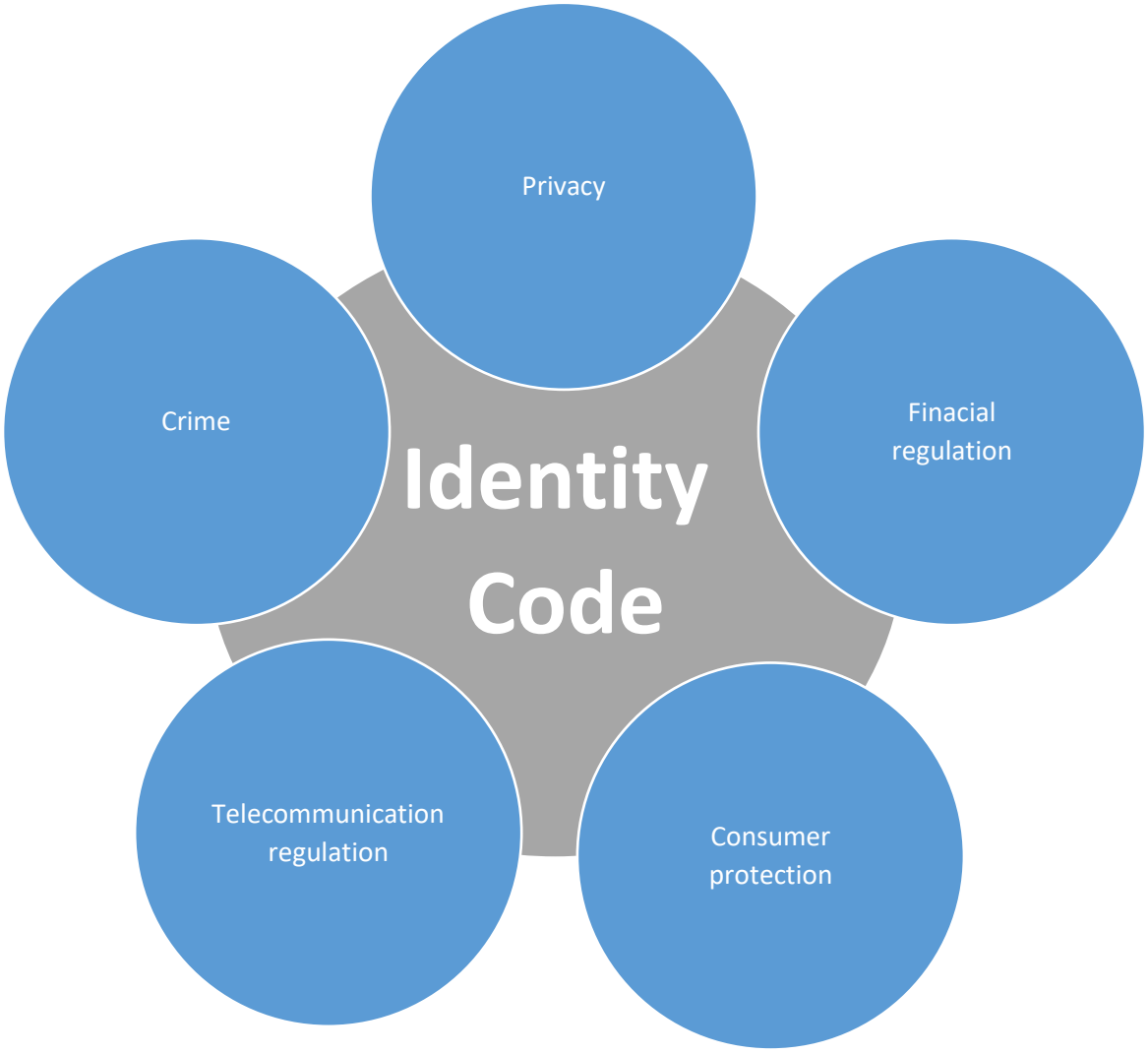
Similarly, with the private sector we envisage that access to the use of DVS and FVS will be the main compliance “lever” available to OIPM.

There will be other laws outside of the IC that mandate high standards of verification, and these will continue to operate. These include such things as working with children, owning a gun, purchasing some pharmaceuticals, undertaking overseas travel. A number of these laws could be simplified by relying on core credentials and FVS.

We recommend that anti-money laundering laws, and laws relating to the issuing and “porting” of telephone numbers should mandate use of core credentials and FVS to identify customers. We also suggest that Consumer Data Rights schemes, designed to promote choice in the financial, energy and telecommunications sectors, mandate a standard approach to verification of identity and mutual recognition through the use of core credentials and FVS.

OIPM should consider having at least some aspects of the IC written as Australian Standards by the standard writers. This could enliven the process of designing and auditing businesses systems to incorporate key IC requirements. It might also be used by the courts and lawyers in determining reasonable standards of conduct by business.

The Identity Code will overlap in some respects with a range of other regulations and regulators.



For example, the requirement of citizen consent is in the Privacy Act and is enforced by the Office of the Australian Information Commissioner (OAIC). There are also State and Territory privacy laws and agencies

In determining how the IC should deal with citizen consent, where aspects of it should sit, and how it should be enforced, there will need to be discussion with the Australian Information Commissioner and her State and Territory counterparts. OIPM might simply

refer complaints or issues about citizen consent; or it might refer more serious cases; or it might jointly investigate some cases with OAIC.

IC itself, might reference to the various laws on Privacy and rely on those; part of IC might be embodied in a new Code under the Privacy Act; IC might set extra and more detailed requirements for citizen consent. These are all possibilities.

The point is that it will be important to figure out how these overlaps are going to be handled, so that businesses and agencies do not have to sort that out for themselves. It is also important that OIPM knows what is going on even if it is not OIPM that is doing it. OIPM needs to have a full and complete view of matters relating to identity.

4. Institutions

The critical institutional change is to establish who is to have overall responsibility for the Australian system of identity. As we observed, no-one is currently responsible for overall Identity policy and practice on identity in Australia.

Office of Identity and Protection Management (OIPM)

We think that this responsibility should sit with an OIPM. To some extent this Office could be constituted from existing resources within Home Affairs. However, it will need extra resources to carry out functions not currently attended to. Importantly, it should also include secondees from the States and Territories. It could also include secondees from the police, the Australian Border Force and national security agencies. It would essentially be a national body, not just a Commonwealth agency.

The main functions of the OIPM should be:

(1) Coordinate overall policy and strategy on identity in Australia.

(2) Set standards and rules including the IC.

(3) Ensure these standards and rules are being complied with, and deal with complaints and problems.

(4) Anticipate, investigate and address emerging issues and problems.

(5) Administer DVS and FVS.

OIPM could sit within Home Affairs. But it needs to function as a truly national Office. So, there should be a "board" or "committee" of Commonwealth and State and Territory officials that oversee the functions and work of the Office, similar to the board of the Australian Criminal Intelligence Commission.

We do not at this stage suggest a legislative base for OIPM nor specific legislated powers. We think that use could be made of multidisciplinary taskforces where there is a need to carry out investigations involving possible criminal or national security issues.

The Office should report to the Ministerial Council for Police and Emergency Management (MCPEM) on its works and sometimes COAG where there is significant "whole of government" matters that require national agreement or approval.

National Registry of Birth, Deaths and Marriages

We recommend certain important things that State and Territory RBDMs should do.

(1) Better exchange information so that there is a single, comprehensive, and accurate record of key life events for every Australian born citizen.

(2) Create a linkage with agencies' "core credentials" so that birth records are "bound" to a biometric, and core credentials are "anchored" to commencement of Identity (see 7.1 above).

The capability of RBDMs is variable. Some jurisdictions simply do not have the resources to put in place the necessary systems. NSW and Victoria have moved toward a "citizen centric", as opposed to a 'transactional' approach to records. They have invested in new systems. Within the constraints of their resources, all the Registrars are trying, to improve the accuracy and integrity of their records, and to improve the exchange of data. For example, they have created a "Fact of Death" file administered by Queensland, which is a comprehensive record of deaths in Australia.

It may be possible to meet our recommendations by similarly cooperating to deal with "change of name" and other life events. However, this is likely to be a complex and huge "high maintenance" solution. We think the time is right for the Premiers and Chief Ministers and the Prime Minister to take a more radical step and set up a National Registry of Births, Deaths and Marriages. This would be a single national registry, which includes a comprehensive record of key life events for every Australian.

This need not detract from the autonomy of States and Territories. It could be administered by a national corporation jointly owned by all jurisdictions[14]. The laws prescribing data to be collected vary at the margins between jurisdictions. These differences should be able to be accommodated. It would probably require Commonwealth assistance to invest in platforms and systems to bring the national system up to the requisite standard, to fit it for the 21st century.

5. Protecting Privacy

We believe that the reforms we propose represent an important piece of public policy to protect the privacy of citizens and consumers. In this section we unpack and explain that contention.

Principle 4 is critical to the effective operation of our proposal.

"PRINCIPLE 4: Privacy and security"

> *The amount of personal data collected and used should be as little as possible and should be stored securely.*
>
> *Except in clearly defined circumstances where it is necessary to access or use the data in the public interest, the consent of the person concerned to the use of the data should be required.*

[14] Similar to Austroads.

We have described the current "system" of identity in Australia as "uneconomical" in the collection and use of identity data. It involves the repeated collection and use of a lot of data and information about people.

Most of this information and data should not need to be collected, and should certainly not need to be retained by most businesses, government agencies and organisations.

The irony is that the proliferation of the collection and use of identity data by multiple players, in an attempt to create greater certainty and security around identity, has exactly the opposite effect. It creates greater opportunities for fraud and "theft" of identity data. It makes the "system" less secure and less reliable.

Central to our solution to this problem is the idea of "skinny identity" which is essentially a biometric and a name and date of birth. That is all that is needed for a robust identity system.

People are sometimes uneasy about the collection and use of biometrics. In our proposal biometric facial images would be collected and retained by a small number of government agencies. The biometric would not be shared with most other agencies or businesses. The only thing that businesses and the majority of agencies would be allowed to do is find out through the FVS whether the face of their customer matches the face the APO has, or the driver licence agency or the visa authority. There is a simple "match" or "no match" answer.

The biometric data collected would not be held in a single data base. FVS would not hold a data base of biometrics, rather it is a hub for directing queries, like a router, across different data sources.

So, this system of reliance effectively limits the amount of data collected and the number of organisations that have the data; in stark contrast to the current system in Australia.

The use of a biometrics also provides a much greater level of security and certainty about a person's identity than the current reliance on a collection of documents. It also makes it

easier and more convenient to check an identity at any point in the process. If there is a very significant transaction or some query or doubts about identity have been raised, then the business or agency can always resort to FVS.

The modern concept of "privacy" increasingly has to do with the idea that people should have control over the use of information about them. It is not only, and sometimes not even, about the confidentiality of information.

A corollary of the idea that people should be able to control information about them, is that they should be informed about the use of that information.

The law, at least in the Australian Privacy Principles, require a person's consent for the use of "sensitive information" which includes biometrics. We also recommend that this requirement, and the right to be informed about the use of identity information should be incorporated into the IC.

We have discussed elsewhere the requirement that the use of facial biometrics and FVS should require a person's choice or consent, or be authorised by law. If that choice is to be a real choice then there will need to be a genuine alternative. That alternative is, effectively, to use the current system of identity in most cases. This might include the use of a document based proofing of identity and the use of the DVS. In high risk situation, it may also include references.

The idea of control has to do not only with the use of information and data and the collection of information and data; we think it also has to do with the broader aspects of identity management. The IC will require businesses to undertake a risk assessment to determine what level of verification and authentication they need to institute. IC should say that they should consult their customers or clients. Increasingly it should be feasible to "customise" security and access to fit the different "risk appetites" of different customers.

The IC will also require the issuers of credentials, including core credentials to take responsibility for managing the consequences of the loss, "theft" or the compromise of

credentials, including core credentials. This will include the "restoration" of the credential. But it may also include helping to put protective measures in place. These measures might include:

1) Where a business or agency thinks a credential has been compromised they should take immediate steps to notify the person concerned (if they are not the source of the information), and the issuer of the credential (if they are not the issuer).
2) Where the possible compromise involved a core credential, they should also inform the Office of Identity Protection and Management (OIPM); and the DVS and FVS should, at least as a temporary measure, place a caveat on the person's identity record, recommending at least that any transaction should include an "in person" check through the FVS.
3) Where there is a reasonable probability that the stolen credential will be misused to obtain credit at the persons expense, then their "credit file" should be put on hold by the credit rating agencies (this would effectively stop institutions from extending substantial lines of credit).

OIPM will be the key agency in ensuring that the IC is complied with. The IC will overlap with many of the existing privacy protections and perhaps the new Notifiable Data Breach Scheme.

There should be consultation with the Office of the Australian Information Commissioner (OAIC) and State and Territory privacy protection agencies to do two things:

1) Consider whether some parts of IC should form a Code issued under the Commonwealth Privacy Act.
2) Decide how complaints relating to privacy should be dealt with where there are overlapping jurisdictions between OIPM and OAIC.

8 Recommendations

8.1 A Federated Approach to Identity

There should be no single agency responsible for identity proofing and no single data base of proved identities.

8.2 A "Skinny" Identity

A person's identity should include a minimal set of attributes, based around facial and potentially other biometrics, name and date of birth details. All other attributes or information should be treated as additional information about a person.

Keeping the concept of identity narrow or "skinny" is important for privacy, interoperability and portability reasons.

8.3 Core credentials

Existing credentials which are biometrically anchored and are of high quality should be defined as core credentials.

The underlying identity proofing and maintenance processes for these credentials should at a minimum meet the new identity management standard (8.4). These credentials include Australian passports, driver licences and ImmiCards. Issuers of core credentials should have an ability to produce basic identity credentials of a comparable high standard that can be provided to members of the public for free.

8.4 A Higher Standard of Reliability – a new Identity Proofing Standard

Core credentials should have a high standard of identity assurance. The Identity Standard should be a central element of a new Code of Identity (8.16) and compliance with the Standard should be enforced and monitored by the Office of Identity Protection and Management (OIPM) (8.19).

The Standard should include requirements:

a) for establishing a facial biometric according to a minimum standard

b) including a process for an in person photograph

c) to carry out a one to many check, to ensure the ID is not duplicated[15]

d) to maintain the accuracy of an identity through periodic renewals of an identity (not > 10 years).

8.5 Reliance on core credentials

As a general principle, and as the basis for a simpler and more efficient system of identity, government agencies and businesses should be able to rely upon core credentials (i.e. passports, driver licences and ImmiCards) for the purposes of verifying and authenticating a person's identity. Government agencies and private organisations should no longer need to rely on the 100 point check.

8.6 Transparency and clarity of reliability for identity credentials

A classification system for the reliability levels of core identity credentials should be developed to provide members of the public, government agencies and businesses with an understanding of the reliability levels of their credentials, and provide an incentive for issuers to improve the reliability of their credentials.

The classification standards should relate to the identity proofing process that was undertaken to establish the identity and issue the credential. It is proposed that a "GOLD", "SILVER", "BRONZE" classification system could be applied with the following minimum standards:

a) Gold standard credentials would be biometrically anchored, would require a one-to-many facial recognition check to be undertaken prior to issuance, and would-be linked to a verified commencement of identity record.

[15] Within the recommendation for a higher standard of reliability, we suggest the use of a one-to-many identification check for the purposes of identity registration. A one-to-many identification check would prevent the registration of duplicate identities within a database and would greatly assist to detect identity fraud. However, we are cognisant that the nature of one-to-many identity checks would result in the disclosure of identities that are intended to be protected. We acknowledge that law enforcement and security agencies have a need to protect the identities of covert operatives and witnesses under protection. For that reason, we have discussed the issue of protected identities with relevant agencies and are confident that existing capabilities and models would be capable of mitigating the risk posed by one-to-many checks.

b) Silver standard credentials would be biometrically anchored and would be linked to a verified commencement of identity record.

c) Bronze standard credentials would not be biometrically anchored, however, documents supporting the claimed identity would need to have been successfully verified through the DVS.

The classification standards would be set by the Office of Information Management and Protection (8.19) and monitored for compliance.

8.7 Rollout of the Face Verification Service

FVS should be completed and rolled out to the private sector at the earliest opportunity. The use of the FVS by the private sector would be contingent upon each organisation meeting standards set out in the Identity Code.

8.8 Requirement for government agencies to use FVS and DVS

All government agencies should use the FVS and DVS to verify or authenticate a person's identity.

8.9 FVS and DVS notifications

The FVS and DVS should be extended to allow notification to a verifying organisation that an individual's credential is at risk of misuse, where there are reasonable grounds to believe a credential has been compromised.

8.10 Privacy and Protection

Existing laws on privacy should continue to apply so that the fact that a person's identity is used by multiple agencies and businesses does not entitle those parties to exchange other personal information about the individual without the consent of that person or for

limited other circumstances (i.e. where an identity has been found to be compromised or used fraudulently).

Further, citizens should be entitled to be informed of how their identity information is being used and shared by businesses and government agencies, with limited exceptions, such as for law enforcement.

Additionally, there should be consultation with the Office of the Australian Information Commissioner (OAIC) and State and Territory privacy protection agencies to do two things:

1) Consider whether some part of the Identity Code should be included under the Commonwealth Privacy Act.
2) Decide how complaints that relate to privacy should be dealt with where there are overlapping jurisdiction.

It should also be mandated that when a Government agency or private organisation becomes aware that identity information or a core identity credential has been compromised, they must notify the person concerned, the issuer of the credential and OIPM.

8.11 Resolution of Identity

Parties that issue a core credential should have the capability to settle problems about the uniqueness or accuracy of that identity. Serious problems may arise where potential questions about the identity cannot for some reason be confirmed – For example, where attributes cannot be verified through the DVS, where there are apparent duplicate identities in the system, or where an individual's face image is unable to be matched through the FVS.

The standards and methodology for the resolution of identity should be set and overseen by the Office of Identity Protection and Management (8.19)

8.12 Vulnerable People

Where someone cannot prove their identity, perhaps because they do not have the required documents or proofs to enrol, there should be a process for proofing their identity as far as possible and issuing them with a credential on the basis of the best information available.

This is likely to be the case for some clients of Department of Human Services and the Department of Home Affairs.

These departments should have the capacity to proof a person's identity and to issue a credential in the same way as other identity providers, observing as far as possible comparable standards of proofing (see 8.4).

8.13 Funding arrangements

Core credentials should be provided to members of the public for free. Consideration should be given to funding the identity system through the application of a fee for use of the FVS and DVS, rather than charging for credentials.

8.14 Consolidating Processes

Governments should consolidate their processes around issuing core credentials and capturing a biometric so that a citizen only needs to attend in person once to get their photograph taken, under ideal conditions.

This process could also include the verification of a person's identity and the issue of a government digital ID.

There would need to be an agreement about the steps in a consolidated process that could be offered to citizens for a passport/driver licence/proof of identity card.

There would need to be agreement about what venues could be used and how they need to be set up.

There would also need to be agreement about the sharing of costs.

8.15 A National Identity Strategy

There should be a new national identity strategy agreed with States and Territories to do the following things:

a) Establish a new higher standard of identity management (8.9).

b) Establish a Code of Identity which will govern the processes of establishing and using identity credentials including digital identities (8.16).

c) Accelerate the roll out of the FVS (8.7).

d) Establish a national Registry for Births Deaths and Marriages (8.20).

e) Establish the State and Territory participation in an Office of Identity Protection and Management to take responsibility for coordination of all aspects of policy and practice in relation to identity (8.19).

f) Establish transition measures to the new identity system.

8.16 A Code of Identity

The new national strategy should include the development of a "Code of Identity" (the IC) that sets out the rules and norms that should govern the management of identity.

The IC should clearly set out the rights and responsibilities of government agencies, businesses, citizens and consumers including:

a) the circumstances under which individuals are entitled to object to the use of or provision of their identity information

b) the circumstances under which individuals are required to identify themselves and how that can be done

c) a positive reporting obligation on agencies and businesses to notify individuals when there are concerns with the security or potential compromise of the individual's identity information

d) redress or remediation processes available to individuals if their identity is misused, stolen or compromised including the obligations and

responsibilities of government agencies and businesses in their role in restoring compromised or stolen identity

e) the rights and obligations of individuals in respect of the use and collection of biometrics.

The IC should set out requirements for:

i. the management of identity – identity proofing, verification, authentication, use, maintenance, restoration and retirement;
ii. practice for the creation and management of biometric templates and data;
iii. the creation and management of physical credentials;
iv. the issuance and management of digital credentials and online identity processes; and
v. protocols for a reliance process – relying upon the fact of an individual's prior identity proofing by another trusted agency such as the APO.

Aspects of the IC could be incorporated into existing legislation relating to privacy and data sharing.

Compliance with the IC should be mandated for all government agencies, including State and Territory agencies, with limited exceptions for law enforcement and security agencies.

Compliance with the IC should be a condition of the use of FVS and DVS by private sector businesses and organisations. Consideration should also be given to having aspects of the IC embodied in an Australian Standard.

Where someone complains that there has been a failure to comply with the IC, the matter should be considered/investigated by the OIPM (8.19) but could ultimately be dealt with by relevant government authorities such as privacy commissioners, information commissioners, consumer affairs departments, ombudsman etc.

8.17 Restoration of Identity

Where a core credential has been compromised, the issuer of the credential must have an agreed process to restore the identity of the victim within their systems and reissue a credential.

8.18 Response to identity compromise

Victim acknowledgement and reporting standards and processes should be developed and applied across the identity system. These standards and processes should be set out in the Identity Code (8.16) to ensure:

a) There is an agreed mechanism for formal acknowledgement of the compromise of an identity and that the individual is at risk of identity misuse. This should replace the identity crime victim certificate regime and allow individuals to determine what organisations or classes of organisations across the identity system they wish to be notified.

b) The rapid transfer of identity compromise information and reporting across the identity system.

In addition, a new provision should be included within the Privacy (Credit Reporting) Code 2014 that requires Credit Reporting Agencies to alert victims of identity "theft" when someone is attempting to access their credit.

8.19 An Office for Identity Protection and Management (OIPM)

A new national OIPM should be established that assumes a lead role and overall responsibility for the various aspects of national identity policy including protection, management and recovery. This could incorporate existing functions, and be located within the Department of Home Affairs and overseen by a national governance board.

The State and Territories should also second members to the OIPM. Functions of the OIPM would include:

a) Establishing and publicising the rules and standards

b) Ensuring compliance with the rules and standards

c) Dealing with complaints and problems

d) Identifying /anticipating emerging problems and trends and keeping the system under review.

e) Administering the DVS and FVS.

Tasks undertaken by the OIPM would include:

i. Development and implementation of a new National Identity Strategy

ii. Development and implementation of an Identity Code

iii. Development and implementation of a new Identity Standard

iv. Completing the roll out of the FVS including to the private sector

v. Development and coordination of strategies to plug key gaps in the identity system in Australia

- Restoration of identity
- Identity resolution

vi. Development of a strategy to address the identity of vulnerable people

vii. Identifying risks and challenges for the system of identity in Australia and developing ways to address these risks and challenges.

viii. Collect and report on key metrics on the performance of the identity system.

ix. Working closely with the National Victim Support Service, IDCARE and any other relevant organisations to support their delivery of frontline response efforts and the point of enrolment for consumers to initiate notification of the compromised identities.

x. Liaise with law enforcement agencies and national security agencies to manage assumed identities.

xi. In due course, take responsibility for the administration of the Commonwealth's digital identity scheme - the Trusted Digital Identity Framework.

8.20 A national Registry for Birth, Death, And Marriage data

Commonwealth, State and Territory Birth, Death and Marriage (BDM) Registries should cooperate to develop a national data exchange so that for every citizen there is a complete comprehensive and accessible record of key life events. This would need to be supported by a reliable reference number system.

We think that there is a strategic opportunity to create a national BDM Registry, which could be owned and operated by a corporation jointly owned and controlled by all jurisdictions.

With adequate resourcing this could be a "step change" in the capability and roles of BDM registries.

8.21 Linking commencement of identity records and core credentials

All individuals should have a commencement of identity record (birth certificate, visa, citizenship certificate) which evidences the commencement of their identity in Australia and anchors other key credentials – i.e. passports, driver licences, proof of age cards etc.

Commencement of identity records should be cross referenced to core credentials and vice versa. For example, a birth record should contain details of what core credentials have been issued to the person. A core credential, like a passport, should contain not only the date of birth, but also the reference number of the relevant birth certificate.

In this way, commencement of identity can be connected to or "bound" to a person's biometric identity, and protected from misuse or "theft".

8.22 Digital identity

The digital ID system for government services (currently known as myGovID) should be developed with a number of modifications. It should:

a) not permit citizens to create multiple IDs in different names

b) mandate the use of the FVS for identity verification when registering for a digital identity credential

c) Allow for the use of the FVS for authentication purposes when accessing services.

8.23 Single digital identity

All governments should agree to the use of a single government digital ID or at least establish a system of "mutual recognition" so that, for example, a Victorian ID could be used to access Commonwealth services.

8.24 Collection of biometrics for immigration and citizenship purposes

The Department of Home Affairs should increase its biometric collection program to collect, at the first possible interaction with the Department, ISO standard facial image biometrics to ensure all identities of those born outside of Australia are biometrically anchored. This will enable subsequent identity verifications or authentications of the individual with other agencies or organisation in future interactions.

8.25 Specific private sector identification requirements

a) The regulated minimum "safe harbour" standards for Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) customer due diligence should be replaced by a requirement to use a core credential and FVS.

b) Improved identity standards should be implemented for carriage service providers which require a facial biometric verification check against a core credential prior to issuing or porting a phone number or undertaking a SIM swapping request.

c) Consideration should be given to mandating the use of core credentials and FVS for the verification of identity by all participants in Consumer Data Rights schemes.

8.26 Additional consumer protections - recommended actions as suggested by the Australian Consumer Competition Commission

There should be consideration given to implementing the range of changes to law suggested by the Australian Consumer Competition Commission including:

i. The creation of larger financial penalties to ensure organisations store data more securely

ii. Providing better protection against the compromise of personal information via mail. This could be through an industry code for the private sector and should include document issuing agencies adopting stronger security conscious practices around the delivery of identity credentials;

iii. Improving resources for victim care providers including:

   a. creating additional grants for individuals and organisations providing remediation, counselling and education services for victims of identity “theft”

   b. providing direct government funding for IDCARE, additional to its current funding model of grants, cost recovered services and member organisation subscriptions. Additional funding would allow for more staff and better support for victims of identity “theft” and related issues

iv. support greater efforts in consumer education about personal information protection across Australia particularly for those who may be disadvantaged and vulnerable.

Appendix 1 – An identity model

A comparison of Identity Management Systems

The Department of Home Affairs commissioned KPMG to develop a model that would provide an indication of the efficacy of the following factors within different identity systems across the globe:

- the integrity and reliability of credentials used to prove identity
- the extent to which those credentials are accepted for the purpose of identity authentiation or verification across society
- the time and cost spent to acquire and maintain identity credentials across a lifetime (labelled as friction).

The model has been used to provide a high level comparison of Australia's current identity system and other systems across the world, as well as to visualise the improvements that would occur within the proposed system.

Caveats

- This model is intended to provide an indication of the integrity, utility and friction levels within identity systems across the globe.
- The data input into the model is taken from open source information in 2018.
- A number of assumptions have been made in terms of the cost time to acquire and renew credentials, average lifespan, and the number of times a citizen may lose a credential in their lifetime.

The proposed Australian system assumes:

- a reliance on a reduced number of high quality photo identification credentials required to prove identity
- the provision of a basic identity credential free of cost to the Australian public

- a recommended higher standard of proofing for core credentials
- the use of biometrics to proof, verify and authenticate identity.

Scoring Factors

Integrity and reliabilty of credentials

The ***Integrity and reliability*** of the system is an average score for all identity credentials reflecting the level of identity proofing activities supporting the issuance of the credential and the security features contained within the credential itself.

Acceptance and use of credentials

The ***acceptance and use of credentials*** within a system is an average score for all identity credentials used within the system relating to how widely accepted the credential is for the purpose of identity verification for life events such as acquiring an education, and receiving healthcare or government benefits.

Friction

The ***friction*** level within a system refers to the average time and cost bourne by individuals to acquire and maintain identity credentials throughout a lifetime, and the cost bourne by government and private industry to verify identity using existing credentials.

Results of the model

The model indicates that the current Australian system has a lower level of integrity and utility, and a higher level of friction than most other countries such as Israel and New Zealand. The lower integrity level within the Australian system is a reflection of the limited use of biometrics to proof, verify and authenticate identity. The lower utility and higher friction levels reflect the large number of credentials in Australia used for identity purposes, and the widespread acceptance of the 100 point check which requires individuals to produce multiple credentials to prove identity.

In the proposed model, there is a signficant improvement in the integrity, utility and friction scores for our identity system, compared with current practice.

Figure 1– A comparison of the integrity identity management systems

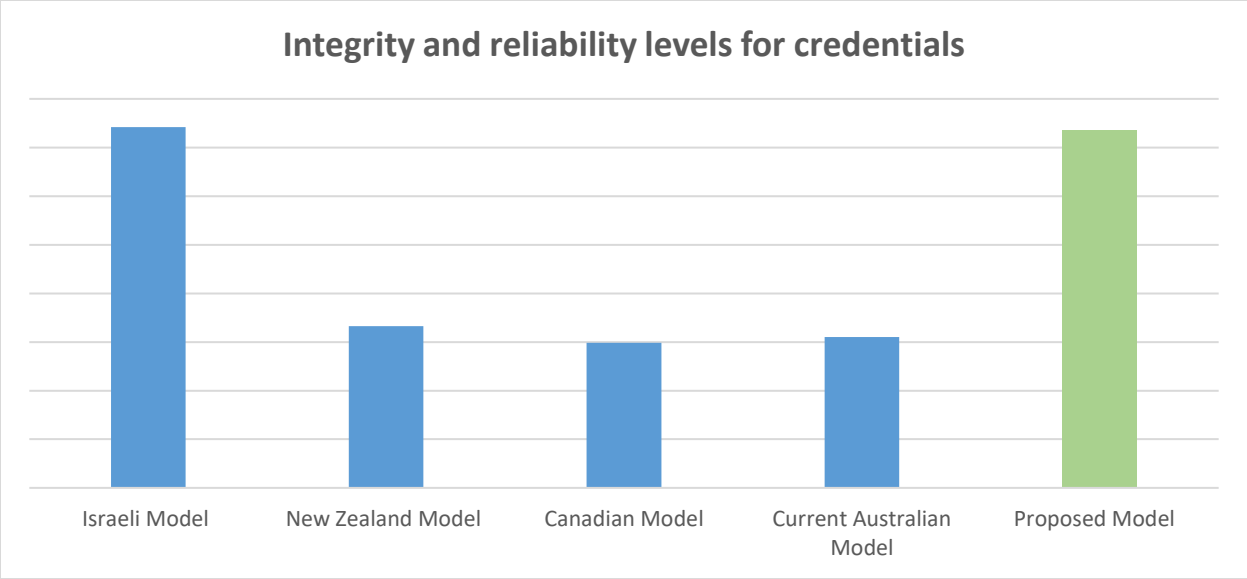


Figure 2 – A comparison of the acceptance and use of credentials in identity management systems

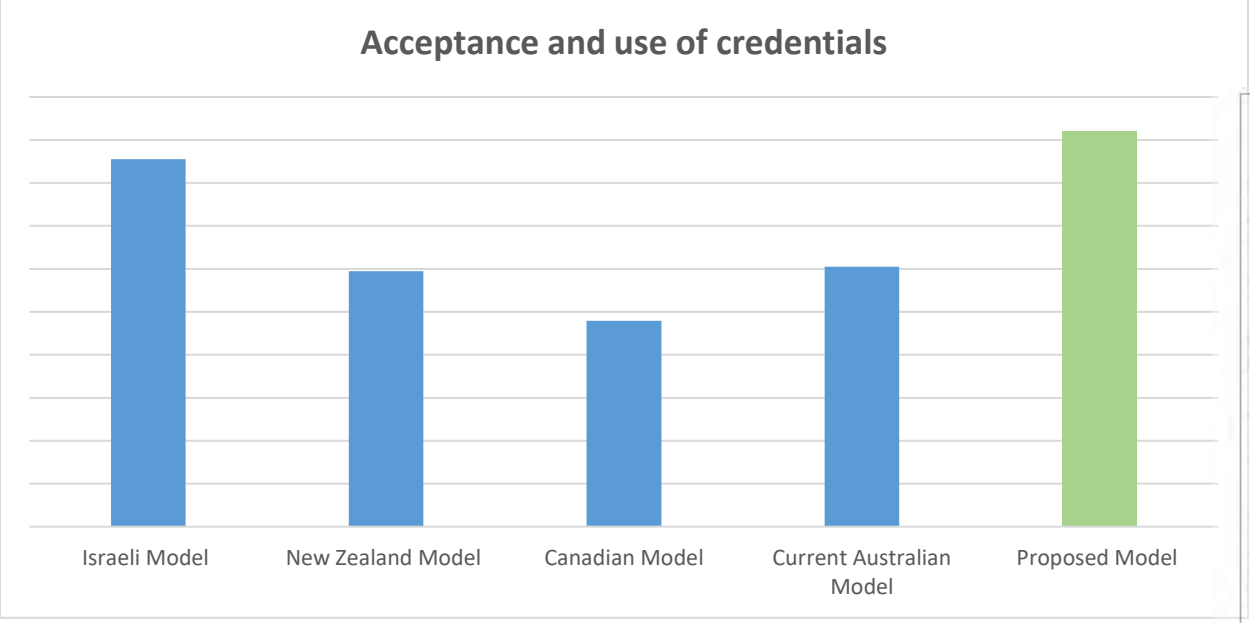
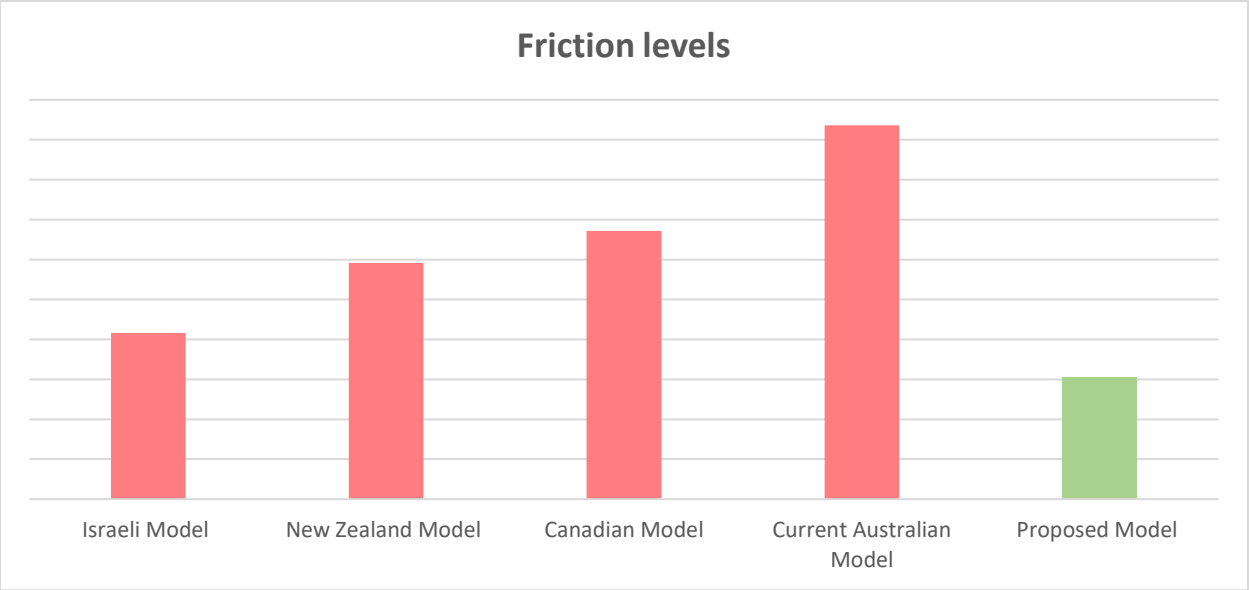


Figure 3 –time and cost of identity management systems



Appendix 2 – Case Studies

s. 37(2)(c)

Project Birrie findings

Fraud and Anti-Corruption Centre

UNCLASSIFIED

Australian Federal Police | Australian Border Force | Australian Crime Commission | Attorney-General's Department
Australian Taxation Office | AUSTRAC | Australian Securities and Investments Commission | Department of Defence
Commonwealth Director of Public Prosecutions | Department of Human Services | Department of Foreign Affairs and Trade

Investigations, intelligence, training, evaluations and quality assurance

Project Birrie

is a multi-agency data-matching initiative led by the AFP-hosted Fraud and Anti-Corruption Centre to examine the nature and extent of criminal offences that were enabled by 1,710 fraudulent identities seized from an organised criminal syndicate in New South Wales. This project represents the first attempt by Australian law enforcement agencies to quantify the impact of fraudulent identity credentials produced by one organised criminal syndicate including how they were used to facilitate other criminal activity.

June – September 2014
DATA CLEANING
- Cleaning and sorting data for matching

September 2014 – March 2015
DATA MATCHING
- Data matching by agencies
- Coordinating, processing and analysing match results

March – September 2015
FINDINGS
- Additional data matching by agencies
- Collating and reviewing findings
- Quality Assurance

OPERATION ARKANIS

An Identity Security Strike Team investigation

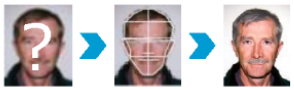
1,710 items of identity information

1,312 images

Biographic matches on false identities

43% of the false identities had at least one match against Commonwealth databases examined.

Facial biometric matches on false identities



As at 1 September 2015 approximately a third of the fake licences had been linked via facial image matching to a real identity, including 35 individuals which held multiple false licences.

Serious and organised crime

Outlaw motorcycle gangs (OMCGs)
13 OMCG members or associates linked to fraudulent licences, including 11 against licences in a name not previously known to law enforcement.

Illicit drugs
29 high profile criminals linked to illicit drug activity.

Fraud
$7+ million losses associated with frauds against individuals and financial institutions.

7 businesses and 1 individual involved in syndicates committing GST refund fraud.

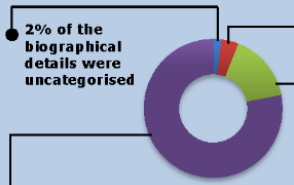
No welfare or passport fraud was detected.

Money laundering
$50+ million in funds transferred offshore.

National security

Threats to national security
A small number of individuals of interest to counter terrorism operations.

SOURCE OF IDENTITY INFORMATION



ADDRESSING VULNERABILITIES

Increased use of the Document Verification Service (DVS)
Use of the DVS by both private sector and government will minimise the ability of criminals to use fabricated identities. As these documents become harder to use, it is likely there will be an increase in identity thefts. Complementing the DVS with a facial recognition capability is integral to ensuring that this risk is minimised.

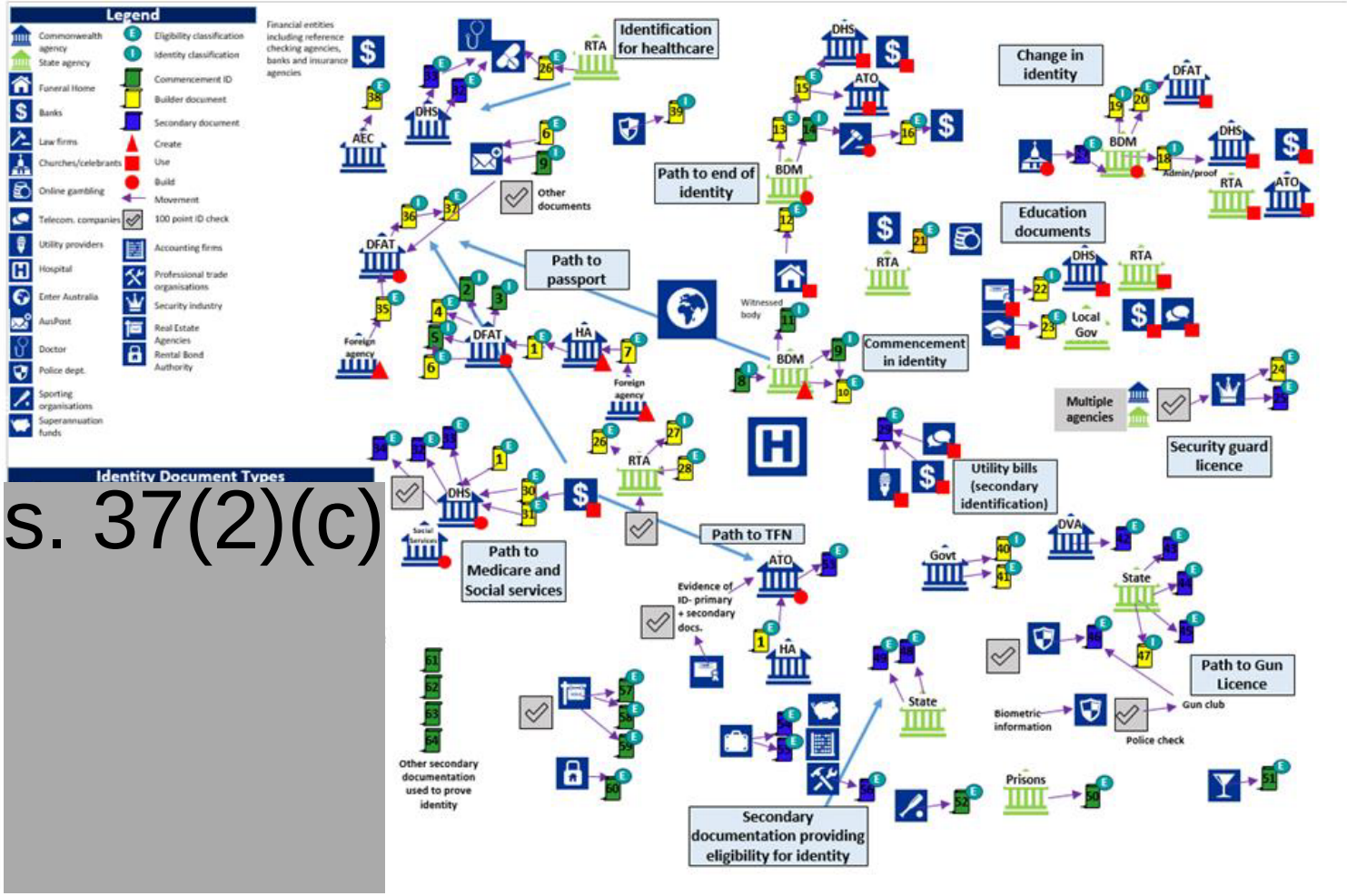
Greater use of facial biometric matching
Use of facial biometrics will provide law enforcement with a powerful tool to identify persons involved in identity crime and other serious offences. However for facial biometrics to provide the greatest available benefit to law enforcement and government, additional reference data sets are required.

Supporting facial biometric capability
Increased use of facial matching as an investigative tool will require appropriate resources including experts trained in facial matching as well as teams to assess and investigate criminality identified through confirmed image matches.

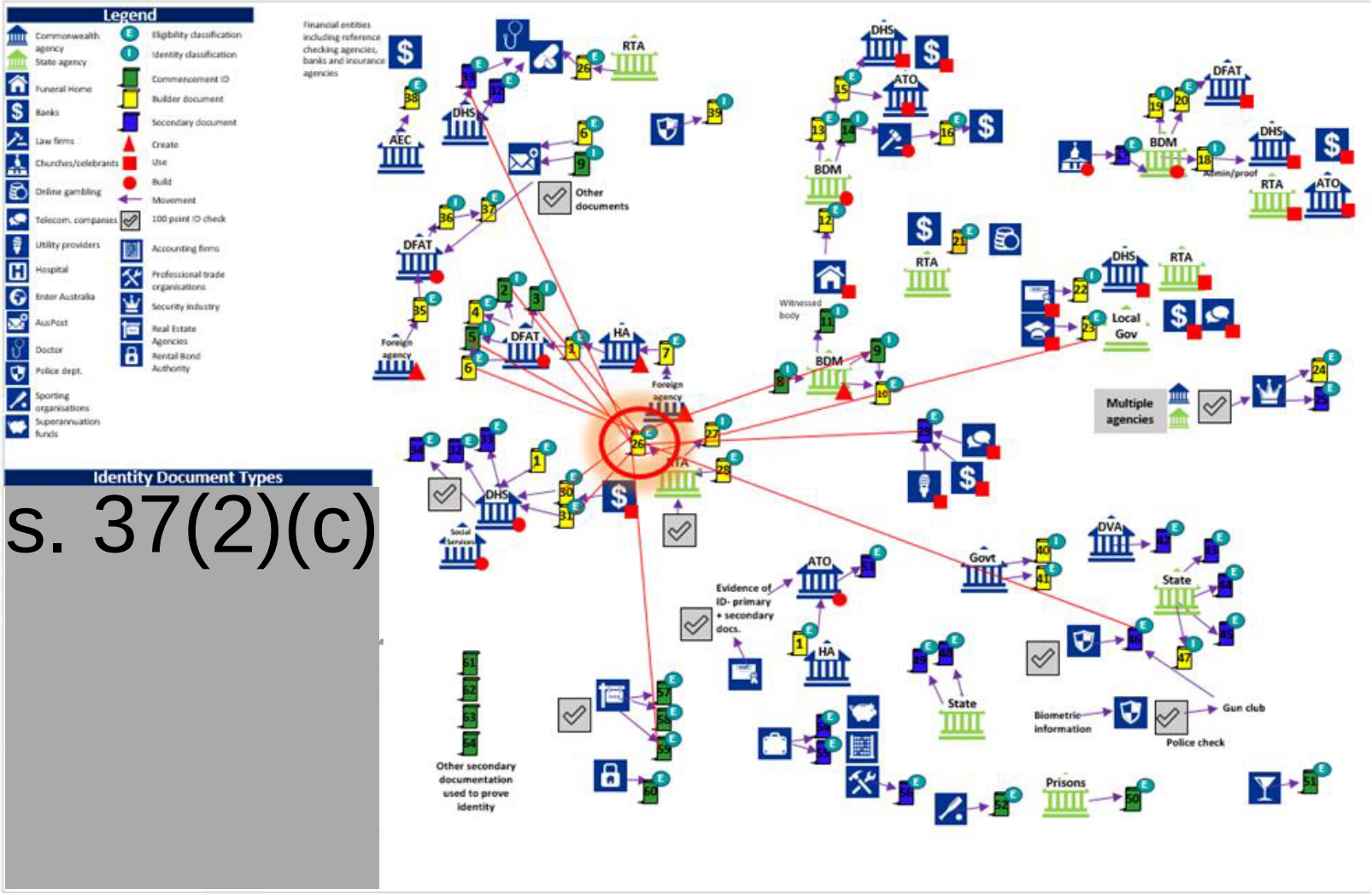
Recording of false identity information
Current law enforcement information systems used by the AFP are not designed to readily record or report on false identity information. Enhanced recording and reporting of false identity information would facilitate better measurement of identity crime and provide significant opportunities for law enforcement.

Appendix 3 – Conceptual map of the Australian Identity System

Conceptual Map of Identity System



Documents Required for Drivers Licence



Appendix 4 – Core credentials

Document	Quality of Biometric Capture	Renewal Period (Years)	Photo Period (Years)	One-to-many biometric check (within organisation environment only)- Issue	One-to-many biometric check (within organisation environment only) – reissue	In person check – issue	In person check – renewal		Recovery[2]
Passport	Biometric ISO/IEC 19794-5	10	10	S. 37(2)(c)					
ImmiCard	Biometric – ISO/IEC 19794-5	3	Undefined (New)						
NSW Driver Licence (1)	Biometric - ISO/IEC 19794-5	10	10.5						
NSW Driver Licence (2)	Biometric - ISO/IEC 19794-5	5	10.5						
QLD Driver Licence	Biometric - ISO/IEC 19794-5	1-5	10.5						
NT Driver Licence (1)	No	10	10						
NT Driver Licence (2)	No	5	10						
WA Driver Licence	Biometric – ISO/IEC 19794-5	5	10						
SA Driver Licence	Biometric – ISO/IEC 19794-5	10	10						
VIC Driver Licence	Biometric - ISO/IEC 19794-2	10	10						
TAS Driver Licence	Biometric - ISO/IEC 39794-5	5	5						
ACT Driver Licence (1)	No	10	11						
ACT Driver Licence (2)	No	5	11						

Appendix 5 – Glossary

Term	Description
100 Point Check	Identification procedures prescribed under in the Financial Transaction Reports Regulations 1990
Authentication	A function for establishing the validity and assurance of a claimed identity of a user, device or another entity by testing the credentials supplied by the person making the claim. This is a process usually required before a person is permitted access to goods, services or assets.
Biometrics	Biological and behavioral characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition
Commencement of identity	Commencement of identity is the first registration by a government agency in Australia and includes RBDM birth registrations and issuance of DIBP immigration documents and records. These may also called cardinal documents.
Core Credential	A credential with a biometric proofed to a high standard and relied on by other. Includes passports, driver licences, ImmiCard and proof of identity cards
Core Identity	Attributes or properties or events that are going to constitute the person's identity such as biometric properties, name and date of birth.

Credential	A Credential is the technology used to authenticate a user's identity. The user possesses the Credential and controls its use through one or other authentication protocols. A Credential may incorporate a password, cryptographic key or other form of secret. To use a digital identity in requesting access to a resource, a subject presents 'Credentials'. The Credentials (once authenticated) are taken as proof that the subject owns the digital identity being presented, and that the subject is permitted to access the resources/services which are associated with their digital identity.
Digital ID	A set of the attributes about a person that uniquely describes the person engaged in an online transaction under the Trust Framework identity ecosystem. Source: TDIF defined term
Document Verification Service	The Document Verification Service (DVS) is a national online system that allows organisations to compare a customer's identifying information with a government record.
Face Verification Service	The Face Verification Service (FVS) is a one-to-one, image-based verification service that can match a person's photo against an image on one of their government records (such as a passport photo) to help verify their identity.
Fact of Death	Compilation of death records from each of the data custodians. These files contain full name, date of birth and residential address details of all the people who have died in Australia.
Federated Identity	A federated system is a decentralised model enabling people to access public and private sector services through a choice of identity provider
Identity	A combination of characteristics or attributes that allow a person to be uniquely distinguished from others within a specific context.

Identity Proofing	Identity proofing is the process of capturing and confirming information to a specified or understood level of assurance to provide organisations with confidence in the identity of a person with whom they are interacting with for the first time.
Identity Resolution	A process for investigating and figuring out a person's true identity where there appear to be multiple identities or no identity
ImmiCards	An ImmiCard is an official identity document issued to certain visa holders who don't have and can't get a passport.
Maintenance	Not a discrete process and comprised of multiple elements including updating core identity, renewing credentials, re-verification of identity including biometric attributes.
National Identity Proofing Guidelines	Strategy document that provides high-level guiding principles to guide identity security initiatives for government and private sector organisations.
National Identity Security Strategy (NISS)	Strategy document developed between Commonwealth, State and Territory governments to develop conditions so Australians may confidently enjoy the benefits of a secure and protected identity.
One Person One Licence	A service that enables a facial image to be compared, on a constrained one-to-many basis, to other images in the National Driver Licence Facial Recognition Solution to identify whether a licence holder or applicant holds multiple licences in the same or a different identity across participating jurisdictions

Registration	Registration is a subset of enrolment. It is the process whereby, having successfully completed the identity proofing process, a person's identity data is recorded.
Reliance	Reliance on a credential issued by another organisation to authenticate a person's identity.
Restoration	A process where a person gets a new credential so they can access their goods, services or assets, particularly in circumstances where a person's credentials have been lost or "stolen" or misappropriated.
Retirement	A process of cancelling an individual's credentials, typically because the person has died.
Skinny Identity	A minimal set of attributes, based around facial and potentially other biometrics, name and date of birth details.
System of Identity	A sequence of processes covering identity proofing, verification, authentication, maintenance, restoration and retirement.
Utility	The ease and expense of getting, using and maintaining a method of proving one's identity.
Verification	The process of checking information (e.g. biometric, name and date of birth) provided at application by comparing it with previously corroborated information (e.g. against the database of the organisation that issued an identity credential). This will assist determining whether a person is the person they claim to be.