



Australian Government

National Strategy for Identity Resilience

Resilient identities – hard to steal, and if compromised, easy to restore.



© Commonwealth of Australia 2023

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

This means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.dpmc.gov.au/government/commonwealth-coat-arms).

Contents

Foreword	2
Data and Digital Ministers Meeting Members	3
Introduction	5
Shared Principles for Resilient Identities	6
Initiatives – Building on existing work and being future ready	9
Short term initiatives (Up to 12 months to implement)	9
Update of the National Identity Proofing Guidelines	9
Cohesive national approach for responding to the identity security aspects of data breaches.....	9
Identity resilience education and awareness	9
Medium term initiatives (1-3 years to implement)	10
Credential Protection Register	10
Mobile phone trust scores	10
Long term initiatives (3-5 years to implement)	10
Reissuing Digital Credentials through Digital wallets.....	10
No wrong doors for identity remediation	10
Strong, consistent commencement of identity records	10
Implementation.....	11
Assessing effectiveness.....	11
Glossary	12

Foreword

Australians need resilient identities - identities that are hard to steal, and if compromised, easy to restore. The National Strategy for Identity Resilience sets out how the Commonwealth, state and territory governments will work together to deliver identity resilience across Australia. It demonstrates our shared commitment to protecting Australians from identity crime and helping them recover when the worst happens.

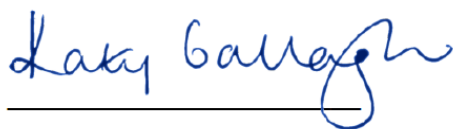
We increasingly rely on the ability to verify our identities - we do this to access everyday services and conduct business. Identity resilience has huge potential as an economic enabler.

However, as the digital economy accelerates, and the world increasingly operates online, Australians' identities are vulnerable in new ways. We need our processes and systems for managing identity information to keep pace with evolving threats by ensuring strong protections and security, centred on the privacy of individuals. We need our identity systems to be inclusive, easy to navigate, and enable safe participation in the economy. A secure and resilient identity system will support broader efforts to keep Australians safe online, including through the development of *the 2023-2030 Australian Cyber Security Strategy*.

Protecting and managing the identity information of Australians is a shared responsibility between the Commonwealth, states and territories. We must all play a role in supporting Australians when things go wrong. Recent data breaches and cyber-attacks highlight the need for a national effort.

The National Strategy for Identity Resilience has been created through close collaboration between the Commonwealth and state and territory governments in the Data and Digital Ministers Meeting. It sets out principles that will provide national strategic direction and practical initiatives that will help protect Australians. The Strategy aligns with efforts to increase cyber security and deliver better services and provides the foundation for strong ongoing partnerships between states, territories and the Commonwealth.

We are committed to creating a secure and trusted digital environment for Australia that enables smarter, safer and more effective service delivery. Together, with state and territory Data and Digital Ministers, we will build a more resilient identity system to underpin the growth of Australia's digital economy, and help to make Australia the most cyber secure nation by 2030.

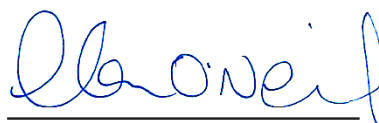


Senator the Hon Katy Gallagher

Minister for Finance

Minister for Women

Minister for the Public Service



The Hon Clare O'Neil MP

Minister for Home Affairs

Minister for Cyber Security

Data and Digital Ministers Meeting Members

Senator the Hon Katy Gallagher (Chair)

Commonwealth

Minister for Finance
Minister for Women
Minister for the Public Service

The Hon Jihad Dib MP

New South Wales

Minister for Customer Service
Minister for Digital Government
Minister for Emergency Services
Minister for Youth Justice

The Hon Danny Pearson MP

Victoria

Assistant Treasurer
Minister for Regulatory Reform
Minister for Government Services
Minister for Creative Industries

The Hon Mark Bailey MP

Queensland

Minister for Transport and Main Roads
Minister for Digital Services

The Hon Stephen Dawson MLC

Western Australia

Minister for Emergency Services; Innovation and ICT; Medical Research; Volunteering

The Hon Andrea Michaels MP

South Australia

Minister for Small and Family Business
Minister for Consumer and Business Affairs
Minister for Arts

The Hon Madeleine Ogilvie MP

Tasmania

Minister for Small Business
Minister for Science and Technology
Minister for Advanced Manufacturing and Defence Industries
Minister for Racing
Minister for Heritage

Mr Chris Steel MLA

Australian Capital Territory

Minister for Transport and City Services

Minister for Skills

Special Minister of State

The Hon Ngaree Ah Kit MLA

Northern Territory

Minister for Corporate and Digital Development

Minister for International Education

Minister for Disabilities

Minister for Multicultural Affairs

Introduction

Australia's digital economy has grown significantly in recent years and continues to grow at a rapid rate, as has the way we use identity. Verifying your identity online, rather than in-person, is increasingly the norm. At the same time, criminals are seeking to steal and misuse identity information and credentials (e.g. driver licence details exposed in data breaches). As a consequence, more Australians are being exposed to cybercrime, fraud and scams.

Identity crime can be enabled by scams which can then facilitate a cycle of further identity and cyber crime. Identity crime is a key enabler of terrorism and of serious and organised crime, the latter of which costs the Australian economy over \$60 billion annually.¹ In 2020-21, Australians reported losing \$33 billion to cyber-crime,² \$1.8 billion was reported lost to scams in 2021 alone, with the unreported figure estimated to be much higher.³

Identity is a combination of characteristics or attributes that allows a person to be uniquely distinguished from other people within a specific context. To prove our identity, we use attributes or characteristics such as our date and place of birth, our address, and increasingly biometrics, such as an image of our face.

Australian governments are committed to working together to make recovery from identity crime simpler and easier for victims. Victims are currently responsible for cancelling their credentials, accounts and services with each government agency, financial institution and private service provider. Each of these entities may have different processes for doing so. This lengthy set of processes increases the distress and frustration of victims, and permits further crime to occur. These difficulties also create a risk that victims will not fully remediate their identity credentials.

Identity crime and recent cyber incidents highlight long-standing issues with identity security and the protection of data in Australia. Australia's approach to identity resilience needs to keep pace with our economic and social activities, and the changing nature of identity crime.

Owing to the federated nature of identity arrangements in Australia, partnerships between states, territories and the Commonwealth are critical. Our best defence is a nationally consistent approach to identity resilience, with all jurisdictions working together on common objectives, standards and practices.

In a 2021 survey on identity crime and misuse, 19 per cent of respondents said they had been victims of identity crime at some point in their life. In 2018-19, identity crime cost the Australian economy \$3.1 billion.

Commonwealth, state and territory governments have a joint responsibility for identity policy. Individuals use a range of credentials to prove their identity, for example, a passport issued by the Commonwealth, and driver licences and birth certificates issued by states and territories. Poor identity security practices in one jurisdiction can be exploited in all the others. Australian governments are committed to achieving consistent national standards across jurisdictions, to build trust and confidence in the identity system.

Australians need resilient identities. A resilient identity is one that is hard to steal, and, if compromised, easy to restore. This requires a consistent national approach. All Australian governments have agreed that the following principles will guide their approach to identity.

¹ Australian Institute of Criminology, Estimating the costs of serious and organised crime in Australia, 2020-21.

² Australian Cyber Security Centre, ACSC Annual Cyber Threat Report, July 2020 to June 2021.

³ Australian Competition and Consumer Commission, Targeting Scams: Report of the ACCC on scams activity, 2021.



Shared Principles for Resilient Identities

PRINCIPLE 1

Seamless Commonwealth, state and territory digital ID systems will support identity resilience

Digital IDs provide a highly secure credential which can be used to prove identity online. They can reduce the amount of information you share, as they allow you to share only the information needed, which means you do not need to share all the details of a valuable identity document such as a passport. Governments will work together to achieve interoperability between digital ID systems and credentials so that Australians can access services in any jurisdiction.

PRINCIPLE 2

Identity needs to be inclusive

Australian governments are committed to supporting vulnerable cohorts to access services, and to supporting Australians that choose not to use digital services or credentials. Indigenous Australians, people from culturally and linguistically diverse communities, and people with disabilities are disproportionately targeted by certain types of scams, and may also have more difficulty accessing or understanding ways to remediate compromises to their ID.⁴ Older Australians are also vulnerable and reported the highest losses to scams in 2021, and may be less likely to adopt digital credentials or other technologies.⁵ Where practical, Australian governments are committed to providing digital and non-digital options so that individuals have a choice in how they manage their identity.

PRINCIPLE 3

Individuals, industry and government have a role to play

Individuals, industry and government all have roles to play in achieving identity resilience. Individuals need to know how to protect their identity and be empowered to proactively respond to identity

⁴ Australian Competition and Consumer Commission, Targeting Scams: Report of the ACCC on scams activity, 2021.

⁵ Australian Competition and Consumer Commission, Targeting Scams: Report of the ACCC on scams activity, 2021.

misuse. Industry and governments can strengthen identity resilience by adopting best practice for preventing, deterring and responding to identity misuse, and by actively coordinating efforts to improve and promote education on identity resilience, secure cyber practices and support services.

PRINCIPLE 4

All jurisdictions will work towards consistent high national standards

Individuals need to have secure and trusted identity credentials regardless of who they are issued by. Australian governments will develop stronger, nationally consistent standards for issuing physical and digital credentials. Australian governments will also ensure that identity credentials have security measures that make them resilient.

PRINCIPLE 5

Biometric establishment and verification of identity with consent can improve resilience

Where appropriate, and with an individual's consent, Australian governments will use biometrics to make it harder for criminals to misuse identity credentials. Combinations of biographic attributes (e.g. name, date of birth and licence number) do not adequately protect Australians from identity crime, and can be exposed in a data breach. Passwords can be forgotten, stolen or compromised. Australian governments will protect personal privacy and secure data in regards to the use of biometrics.

PRINCIPLE 6

All jurisdictions will allow an individual to update their information conveniently across agencies

Currently, an individual who changes their name or moves house has to update each credential individually, and often does not. As a result, their personal details may differ between government agencies and jurisdictions, which increases the potential for identity fraud. Australian governments will work towards enabling individuals to update their credentials in a more streamlined and convenient way, if the individual wishes to do so.

PRINCIPLE 7

Less data collection and retention

Large data breaches have demonstrated the risks associated with large stores of personal information and of retaining copies of credentials. We need to consider the likelihood of future data breaches when deciding what we collect and retain. Digital IDs, digital credentials and government services like the Document Verification Service, allow government agencies and businesses to verify identity while minimising their collection of personal information. Australian governments will support businesses and government agencies to collect and retain less personal information where appropriate. This will be balanced against existing and legitimate needs relating to law enforcement and regulatory regimes.

PRINCIPLE 8

Clear data-sharing arrangements

To support individuals impacted by large scale cyber incidents and data breaches, governments need to be able to collect and share data. Australian governments will work to put in place data-sharing arrangements to better protect victims of cyber incidents and data breaches.

PRINCIPLE 9

Consistent revocation and re-issuance

Across Australia there are different processes for revoking and reissuing credentials. This makes it harder for a victim of identity crime to recover, especially when they have to engage with multiple Commonwealth, state and territory agencies and the private sector. Australian governments will work towards streamlined and consistent processes for remediating compromised identity credentials to reduce the burden on victims.

PRINCIPLE 10

Clear accountability and liability

Liability for the cost of remediating credentials compromised in a data breach, cyber-attack, or other identity crimes needs to be clear, along with appropriate enforcement actions. The lack of clear accountability can delay mitigation measures when responding to a data breach. The solution should minimise further harm to the individual whose data was compromised.

Initiatives – Building on existing work and being future ready

To give effect to the above principles, Australian governments have committed to the following short, medium and long term initiatives. Plans for implementing the initiatives will be considered by the Data and Digital Ministers Meeting. The Data and Digital Ministers Meeting, a sub-committee of National Cabinet, will also oversee the implementation of the initiatives.

Building on the innovative and leading edge work of the Commonwealth, states and territories, the initiatives include the elevation of existing projects to the national stage. They complement initiatives that support identity resilience, which are in development or already in operation, but have not been included in this Strategy. These include, for example, the Commonwealth's myGov and myGovID systems, the Trusted Digital Identity Framework, ID Support NSW, and the Australian Death Check.

Short term initiatives (Up to 12 months to implement)

Update of the National Identity Proofing Guidelines

Australian identity proofing standards need to be fit for purpose and used consistently across the country. The National Identity Proofing Guidelines (the Guidelines) provide guidance for government and private sector organisations on proofing the identity of individuals. The Guidelines will be updated and aligned with the Trusted Digital Identity Framework to support consistent processes across digital and non-digital credentials. This will help to address longstanding inconsistencies in identity management practices between jurisdictions; support less collection and retention of data; and build confidence in the use of Commonwealth, state and territory digital ID systems.

Cohesive national approach for responding to the identity security aspects of data breaches

Large-scale data breaches and cyber incidents have demonstrated the need for a cohesive national response to the identity security aspects of data breaches, to minimise the damage caused and to expedite the recovery of individuals' identities. This initiative will seek to establish a Centre of Excellence to increase the speed and efficiency of responses to the identity security aspects of significant data breaches. This will be a single and highly visible point of expertise that supports the management of the identity security aspects of breaches at a Commonwealth level, and works with state and territory bodies, to minimise the harm for individuals, businesses and governments.

Identity resilience education and awareness

Education and awareness can help build individual, industry and government resilience. A range of education and awareness programs exist across the Commonwealth, states and territories. These include the Australian Competition and Consumer Commission's Scamwatch and awareness information delivered by ID Support NSW. Improving consistency and coordination at a national level will increase the effectiveness of these programs. This initiative will focus on amplifying and coordinating existing education and awareness efforts to better protect Australians.

Medium term initiatives (1-3 years to implement)

Credential Protection Register

When a credential is discovered to have been compromised it can take a long time to remediate. During this time, criminals can continue to misuse the credential. In October 2022, the Commonwealth established the Credential Protection Register to prevent the Identity Matching Services verifying a compromised credential that has been listed on the Register. This initiative will seek to further develop the Credential Protection Register, for example to allow individuals to have better control of their credentials, and also to improve the sophistication of the Register.

Mobile phone trust scores

Mobile phone numbers can be integral to identity authentication (for example when used in multifactor authentication) and as an alternative to using email and social media to contact a client. However, they can also be used for identity takeover and fraud. A 'Mobile phone trust score' system would allow telecommunication providers to assign trust scores to mobile phone numbers based on risk factors such as recent sim swaps, tenure of phone plan and virtual private numbers. The trust score will help to prevent mobile phones being used to facilitate fraud.

Long term initiatives (3-5 years to implement)

Reissuing Digital Credentials through Digital wallets

Digital Credentials (for example Working with Children Checks or mobile driver licences) are important for identity resilience. It is cheaper, easier and quicker to reissue a digital version of a compromised credential than a physical one. The development of digital credential standards is vital to ensure consistency of data, user experience and interoperability, while maintaining choice and privacy. This initiative will look at addressing technical and legislative differences and barriers across jurisdictions to help reduce fraud, improve customer experience and reduce duplication of effort. This initiative can also inform upcoming digital credential projects so that they are ready for digital wallets at launch.

No wrong doors for identity remediation

Individuals should be able to engage with one government organisation in order to fully and quickly recover their identity. This could include regaining control of online accounts, revocation and re-issue of credentials, and protective measures for compromised credentials. Some states and territories have already established comprehensive support services that operate within their jurisdiction. This initiative will focus on a cross-jurisdictional approach to improve the experience for individuals, reduce further harm and enable full identity recovery.

Strong, consistent commencement of identity records

Commencement of identity records such as birth certificates, and immigration records for Australians born overseas, are issued by different jurisdictions and are not always linked to change of identity (e.g. change of name) processes in other jurisdictions. This initiative will explore how jurisdictions can work together to improve the integrity of identity records, and provide every Australian with an accurate commencement of identity record updated for life events.



Implementation

Realising the intent of the Strategy will require a strong focus on cross jurisdictional collaboration, application of the principles, and the implementation of the initiatives. Under the oversight of the Data and Digital Ministers Meeting, and in close collaboration with all Australian governments, the Commonwealth, through the Department of Home Affairs, will coordinate the implementation of this Strategy.

A detailed plan, including resources required, will be developed for each initiative for consideration and approval by the Data and Digital Ministers Meeting.

Assessing effectiveness

In implementing this strategy, effectiveness will be assessed by progress made towards implementation of the initiatives, and the effectiveness of these outcomes. An annual report will be provided to the Data and Digital Ministers Meetings on the effectiveness of the Strategy, associated policy and legislation, and follow-on actions required to ensure that Australians' identities are resilient.

The 2023 National Strategy for Identity Resilience replaces the 2012 National Identity Security Strategy.

Glossary

Attribute	A characteristic that can be used (in combination with other attributes) to uniquely identify a person in a specific context (such as name, date of birth or a unique number).
Authentication	A function for establishing the validity and assurance of a claimed identity of a user, device, or another entity by testing the authenticators supplied by the person making the claim. This is a process usually required before a person is permitted access to goods, services or assets. Examples of authenticators include passwords, fingerprint ID and security questions.
Biographic attributes	Information relating to a person's life, such as their name, date of birth and licence number.
Biometric Information	Information about any measurable biological or behavioural characteristics of a natural person that can be used to identify them or verify their identity, such as face, fingerprints and voice. Biometric information includes biometric templates. (Under the Privacy Act 1988, biometric information is considered sensitive information, which provides additional obligations on organisations).
Credential	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 include an identity document that contains or incorporates identification information and that is capable of being used as evidence of identity. For example a driver license and or passport.
Commencement of Identity' Documents	Commencement of identity is the first registration by a government agency in Australia and includes Registers of Births, Deaths and Marriages and issuance of the Department of Home Affairs' immigration documents and records.
Compromised Identity	Where an individuals' credentials, including digital ID have been lost, stolen, damaged or duplicated without authorisation. This also includes identity information that has been exposed in a data breach.
Data Breach	Loss or misuse of, unauthorised access to, or unauthorised modification or disclosure of, personal information held by an entity.
Digital Credential	A digitised version of a credential, for example a digital driver license.
Digital ID	A distinct electronic representation of an individual which enables that individual to be sufficiently distinguished when interacting online with services. A Digital ID may include attributes which are bound to a credential.
Document Verification Service	A national real-time system that allows participating organisations to compare a customer's identifying information on particular government issued documents with the issuing government agency. The DVS is a secure system that operates 24/7 and matches key details contained on Australian-issued identifying credentials providing a 'yes' or 'no' answer within seconds.

Identity	A combination of characteristics or attributes that allow a person to be uniquely distinguished from others within a specific context.
Identity Crime	Activities or offences in which a perpetrator uses a fabricated, manipulated, stolen or otherwise fraudulently assumed identity to facilitate the commission of crime.
Identity Fraud	The gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated, manipulated, stolen or otherwise fraudulently assumed identity.
Identity Resilience	Making identity hard to steal, and if compromised, easy to restore.
Interoperability	The ability of identity systems operated by different jurisdictions to exchange, accept and make use of information.
National Identity Proofing Guidelines	These guidelines provide guidance for government and private sector organisations on proofing the identity of individuals.
Personal Information	Includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances. Personal information may include: an individual's name, signature, address, phone number or date of birth
Proofing	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 for the first time.
Remediation	The process of recovering and restoring an identity that has been compromised.
Revocation	The act of recalling and cancelling a physical or digital credential or digital ID that has been compromised.
The Trusted Digital Identity Framework (TDIF)	An accreditation framework for digital ID services. It sets out the requirements that applicants need to meet to achieve accreditation including (but not limited to) privacy, fraud and security control, accessibility and usability, system testing, risk management, identity proofing and credential management. The TDIF also includes guidance material and templates to support applicants to meet TDIF requirements.
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 authenticator). This will assist in determining whether a person is the person they claim to be.

