Australian Government
Office of the Australian Information Commissioner

Office of the Australian
Information Commissioner

Digital ID regulatory strategy

Last edited: 18 December 2024

OAIC

The Office of the Australian Information Commissioner (OAIC) was established on 1 November 2010 by the *Australian Information Commissioner Act 2010*.

ISSN 2202–7262

Creative commons

Contact

Enquiries regarding the licence and any use of this strategy are welcome.

Online: Submit an Enquiry form
Website: oaic.gov.au
Phone: 1300 363 992
Monday to Thursday
10 am to 4 pm (AEST/AEDT)

Mail: Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

Non-English speakers

If you speak a language other than English and need help, please call the Translating and Interpreting Service on 131 450 and ask for the Office of the Australian Information Commissioner on 1300 363 992.

Accessible formats

All our publications can be made available in a range of accessible formats. If you would like this report in an accessible format, please contact us.

Contents

Digital ID regulatory strategy

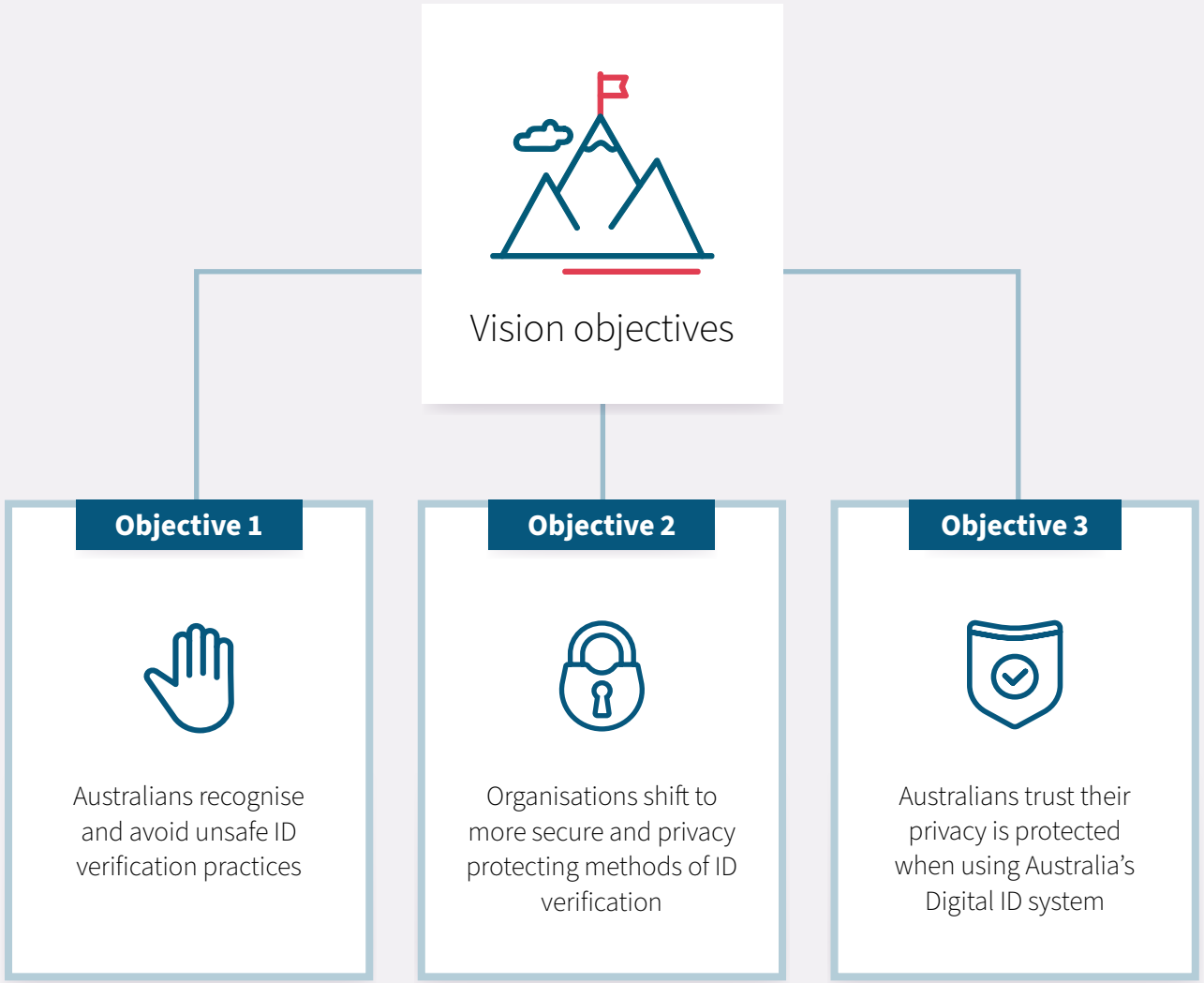
The OAIC is the independent national regulator for privacy and freedom of information. Our purpose is to promote and uphold individuals' rights to access government-held information and protect their personal information.

As the privacy regulator of Australia's Digital ID System and other APP identity-related entities, the OAIC is responsible for ensuring individuals' privacy is protected when using accredited Digital ID services and other identity-related services.

The OAIC has created a theory of change-based Regulatory Strategy that explains how the activities undertaken will contribute to our vision as privacy regulator of Australia's Digital ID System and other APP identity-related entities. The Digital ID regulatory strategy describes how the OAIC proposes to use its regulatory powers to build trust and confidence in Australia's Digital ID System and make ID verification in Australia more secure and privacy protective.

'The OAIC is responsible for ensuring individuals' privacy is protected when using accredited Digital ID services and other identity-related services.'

Vision


Vision objectives
Objective 1
Australians recognise and avoid unsafe ID verification practices
Objective 2
Organisations shift to more secure and privacy protecting methods of ID verification
Objective 3
Australians trust their privacy is protected when using Australia's Digital ID system

Our vision as privacy regulator of Australia's Digital ID system and as privacy regulator of entities that routinely verify individuals' identity ensures:

Objective 1

Australians recognise and avoid unsafe ID verification practices.

- The OAIC's activities are designed to raise public awareness about safe methods for verifying ID online. By providing consumer focused resources, the OAIC aims to help individuals understand the types of issues they can report and their rights in relation to privacy.
- Enforcement actions and targeted communications will further educate the public on secure ID verification practices, supporting the broader vision of Australians confidently recognising and avoiding unsafe verification methods.

Objective 2

Organisations shift to more secure and privacy protecting methods of ID verification.

- The OAIC seeks to engage with organisations to emphasise the importance of adopting safe identification practices, including the benefits of becoming a relying party within Australia's Digital ID System. This shift aims to reduce the unnecessary circulation and retention of personal information online.
- In the short term, the OAIC aims to build organisations' skills, education and awareness of privacy standards. Over time, these efforts aim to lead to improved privacy practices, stronger data handling standards, and more secure methods for managing identity documents. Encouraging organisations to minimise unnecessary data retention and partner with accredited Digital ID providers will contribute to the OAIC's vision of a safer and more privacy protective identity verification landscape.

Objective 3

Australians trust their privacy is protected when using Australia's Digital ID system.

- The OAIC activities, such as the provision of privacy guidance for accredited entities, aims to ensure these entities have the necessary information to comply with legislative requirements. Activities such as investigations, enforcement actions and transparent communication of outcomes will reinforce public trust and highlight the OAIC's role as the privacy regulator.
- By conducting other activities such as assessments of accredited entities' privacy practices, the OAIC seeks to address harms associated with the mishandling of identity information. These efforts will ensure accredited entities uphold high standards of privacy, contributing to the broader vision of Australians trusting that their privacy is protected when using Australia's Digital ID System.

Digital ID theory of change

This theory of change outlines the OAIC's approach as Digital ID privacy regulator. The remainder of this document steps out key elements of this approach in more detail.

Digital ID enables secure, convenient, voluntary identity verification, enhancing trust in digital systems and shifting Australians away from unsafe identity verification practices.

OAIC activities

To achieve our vision, the OAIC will adopt a whole of system approach to regulation, with a focus on the following activities:

Educate

Encourage compliance with the law, and encourage Australians and businesses to shift to more secure means of ID verification.

Monitor

Anticipate and detect non-compliance through gathering intelligence and monitoring trends, to inform our compliance and enforcement priorities and identify possible areas for investigation

Enforce

Enforce privacy safeguards, including resolution of possible breaches through investigation, litigation and other formal enforcement outcomes

Deter

Ensure visibility of our regulatory actions and communicating compliance outcomes

Collaborate

Build strong relationships with the regulated community, industry and government

Indicative activities

Through a range of activities, we will target actions and initiatives that reflect our regulatory strategy and focus areas. Below are some indicative activities that may be undertaken over the first three years of the Digital ID program. The delivery of the full range of activities proposed below is dependent on the scope of the OAIC's continuing role as privacy regulator of Australia's Digital ID System.

		Year 1	Year 2	Year 3+
Activity 1	Undertaking targeted stakeholder engagement with consumer groups and system participants to promote Digital ID as a privacy protecting initiative.			
Activity 2	Support consumer groups to develop education materials and campaigns on secure ID verification			
Activity 3	Engaging with other agencies in the Digital ID program to ensure privacy is protected during the system's expansion			
Activity 4	Organising stakeholder education workshops & materials for peak bodies/APP entities on privacy obligations & Digital ID safeguards			
Activity 5	Providing guidance and education to accredited entities on managing notifiable data breaches			
Activity 6	Proactively applying enforcement powers to issue infringement notices, injunctions and civil penalty provisions			
Activity 7	Integrating Digital ID into Privacy Attitudes Survey			
Activity 8	Undertaking assessments of accredited entities to build trust in the Digital ID privacy safeguards including:			
	a. Assessing key risks and existing accredited entities			
	b. Assessing State and Territory participating entities			
	c. Assessing private sector participating entities			
Activity 9	Undertaking assessments and other regulatory actions targeted to ensure identity-related services operating outside Australia's Digital ID System comply with the APPs			
Activity 10	Proactively communicating guidance and outcomes from complaints, assessments, investigations and determinations			
Activity 11	Handling enquiries and complaints			

Outcomes

Short-term outcomes

In the short term, the OAIC's activities are expected to produce the following outcomes.

Mature existing awareness about privacy across multiple domains of life

Individuals will develop a more nuanced understanding of privacy issues recognising their significance across various aspects of their lives, including personal, professional, and social domains. This heightened awareness will lead to more informed decisions and proactive measures to protect personal data.

Privacy laws actively enforced to address harms linked to mishandling of identity information

Privacy laws will be rigorously enforced and address harms resulting from the mishandling of identity information. This active enforcement will ensure accountability and provide a deterrent against negligent or malicious data practices.

Digital services culture supports quality improvements in cyber security and privacy practices

A proactive approach to quality improvement will foster a cultural shift aimed at encouraging continuous enhancement and adherence to best practices, leading to safer and more reliable digital experiences for Digital ID users.

Organisations develop skills, education and awareness on privacy practices and obligations

Organisations will invest in developing the necessary skills, education, and awareness among staff regarding their privacy obligations. This commitment to training and knowledge will ensure that employees are well-equipped to handle data responsibly and in compliance with regulatory requirements and industry best practice.

Long-term outcomes

In the longer term, the OAIC's activities will support the following outcomes.

All organisations enhance their privacy compliance practices and transparency

Organisations across various sectors will implement robust privacy measures, ensuring data protection practices are consistently updated and transparent. This enhancement will foster trust and compliance, aligning with high standards of data security and user privacy expectations.

Public understands Digital ID and the OAIC's role as the privacy regulator

Through targeted education and outreach initiatives, the public will gain a comprehensive understanding of the privacy benefits offered by the program and the role of the OAIC as privacy regulator. The knowledge will empower individuals to make informed decisions about their digital interactions and trust in regulatory oversight.

Individuals expect high quality cyber security practices from digital services

As awareness of cyber security issues increases, individuals will demand and expect digital services to adhere to a high level of cyber security practice. This shift will drive service providers to prioritise and enhance their security measures to meet individuals' expectations.

Organisations encouraged to use more secure practices

Organisations will be motivated to adopt more secure practices, ensuring that data protection becomes a standard part of their operational protocols. This encouragement will lead to a more resilient digital ecosystem, reducing vulnerabilities and enhancing overall security.

Organisations adopt privacy enhancing practices and cyber security training

Organisations that handle identity documents will adopt privacy enhancing practices and cyber security initiatives, ensuring they have the necessary resources to implement and maintain high data protection standards.

Enhanced data handling industry standards

Industry standards for data handling will be elevated, setting a new benchmark for how data is collected, processed, and stored, with data minimisation as the starting point rather than an end goal. These enhanced standards will ensure consistent application of best practices across industry, improving trust and security in digital services.

Impacts

Our intended impacts

The OAIC aims to realise the following impacts through its activities and as a combined result of the above outcomes:

- Accredited entities are confident they have the information they require to comply with legislation
- Accredited entities consistently uphold quality privacy practices and demonstrate compliance with all relevant legislation
- Improved privacy practices amongst organisations that handle identity documents
- All organisations that handle identity documents consistently uphold quality privacy practices and adhere to enhanced data handling industry standards
- Individuals make informed choices about the handling of their identity information

Regulatory focus areas

The OAIC seeks to detect trends early and focus on escalating persistent and systemic trends for potential regulatory action to mitigate harm.

Based on the OAIC's assessment of high-risk areas, the OAIC will monitor the industry in relation to user profiling, data retention, consent, law enforcement requests, biometric information and consumer privacy rights as they relate to Digital ID. The OAIC will also monitor and mitigate risks arising from unsafe ID verification services for all organisations.

Specifically, we will focus our proactive regulatory efforts on the following areas, noting that all activities are indicative and will evolve to meet the needs of Digital ID program implementation.

Biometric information

Example activities

- **prioritise complaints** regarding biometric information
- **analyse and report** systemic trends to inform compliance and enforcement options

Law enforcement access

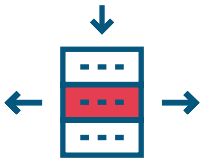
Example activities

- **conduct assessments** on requests made by law enforcement bodies and the information provided by recipients to ensure compliance
- **provide guidance** on when entities may disclose personal information to law enforcement bodies

Express consent

Example activities

- **provide guidance** on express consent for accredited entities
- **educate consumers** on their rights regarding express consent through consumer group engagement
- **enforcement action** to deter poor consent practices



Data retention

Example activities

- **provide guidance** on retention periods for Digital ID related information
- **conduct assessments** on the retention of non-biometric data in larger accredited entities

ID Verification*

Example activities

- **conduct assessments** on entities already providing identity verification services
- **enforcement action** against poor identity verification practices
- **publicise regulatory action** and outcomes to improve awareness of unsafe identity verification practices

*unaccredited ID services

oaic.gov.au
corporate@oaic.gov.au