Australian Government
Department of Home Affairs

Digital ID Act 2024

Annual Report 2024-25

Table of Contents

Executive Summary

Section 155B of the *Digital ID Act 2024* (the Act) requires that each year, the Australian Federal Police (AFP) Minister table in each House of Parliament a report on the use and disclosure of personal information (including biometric information) for law enforcement purposes, by entities accredited under the Act (an accredited entity).[1]

The report is required to set out the extent and circumstances in which law enforcement agencies and enforcement bodies request or require an accredited entity to disclose personal information (including biometric information), where that information was obtained by the accredited entity from the provision of the entities' accredited services.

This inaugural report captures requests made by law enforcement agencies and enforcement bodies between 30 November 2024 and 30 June 2025. The Australian Taxation Office (ATO) was the only agency identified as having reporting obligations for the relevant period.

Reporting by law enforcement agencies under the Digital ID Act

The Act establishes a secure, convenient, voluntary and inclusive way for verifying identities online, enabling individuals to interact with government and businesses safely while ensuring strong privacy protections for their personal information.

The Act creates an accreditation scheme for Digital ID service providers and sets out the principles, governance, and oversight mechanisms for the regulation of entities providing or relying on Digital ID services.

Section 155A of the Act imposes reporting obligations on law enforcement agencies and enforcement bodies, including state and territory agencies, that request or require an accredited entity to disclose personal information (including biometric information) that the entity obtained in the provision of its accredited services.

At the end of the financial year, impacted law enforcement agencies and enforcement bodies are required to provide the AFP Minister with a report by 30 September, including:[2]

- the total number of requests or requirements made during the financial year,
- details of the type of information requested or required (but not identifiable personal information) during the financial year, and
- the total number of request or requirements that were complied with (in whole or in part) by an accredited entity during the financial year.

Under section 155B of the Act, the AFP Minister is subsequently required to prepare a consolidated report based on the provision of reports under section 155A of that Act and to table that report in both Houses of Parliament within 15 sitting days of completion.

The primary purpose of the reporting is to strengthen transparency over law enforcement agencies and enforcement bodies access personal information (including biometric information) in Australia's Digital ID System. The reporting allows monitoring of what kinds of personal information (including biometric information) are being disclosed and accessed for law enforcement purposes, and the frequency and appropriateness of requests for information and associated disclosures.

---

[1] Since the release of the 2025 Administrative Arrangement Orders, the Minister of Home Affairs presides as the AFP Minister.
[2] Or by the end of any further period granted under subsection 34C(5) of the *Acts Interpretation Act 1901*.

Use and disclosure of personal and biometric information

Personal and biometric information, collected for the provision of accredited services by an accredited entity, may only be disclosed to a law enforcement agency or an enforcement body under certain circumstances, with stricter disclosure requirements for more sensitive biometric information.

Section 49(3) of the Act provides that an accredited entity is authorised to disclose biometric information of an individual to a law enforcement agency if one of following circumstances apply:

- disclosure is required or authorised by or under a warrant issued under a law of the Commonwealth, a state or a territory, or
- the accredited entity has the express consent of the individual, and the disclosure is for the purpose of verifying their identity or investigating or prosecuting an offence against a law of the Commonwealth, a state or a territory.

Enforcement bodies that possess powers to request or compel information but do not have access to warrant powers will not be able to access biometric information where this is held by an accredited entity, unless the individual's express consent is provided.

Section 54 of the Act provides that an accredited entity must not use or disclose personal information that is not biometric information, for the purposes of enforcement related activities conducted by, or on behalf of, an enforcement body, unless one of the following circumstances apply:

- the accredited entity is satisfied that the enforcement body has started proceedings against a person for an offence against a law of the Commonwealth, a state or a territory, or a breach of a law imposing a penalty or sanction,
- the disclosure is required or authorised by or under a warrant issued under a law of the Commonwealth, a state or a territory,
- use or disclosure of the information is for the purposes of reporting a suspected or actual digital ID fraud incident or suspected or actual cyber security incident,
- the information is used or disclosed by the accredited entity for the purpose of complying with the Act, or
- the accredited entity has the express consent of the individual (to whom the personal information relates), and the disclosure is for the purpose of verifying their identity, or investigating or prosecuting an offence against a law of the Commonwealth, a state or a territory.

Under the Act, use and disclosure of personal and biometric information must be reported on by:

(a) a law enforcement agency, if the agency requests or requires, during a financial year, an accredited entity to disclose biometric information of an individual obtained as part of the provision of the entity's accredited services, or

(b) an enforcement body, if the body requests or requires, during a financial year, an accredited entity to use or disclose personal information of an individual obtained as part of the provision of the entity's accredited services for the purposes of enforcement related activities conducted by, or on behalf of, the enforcement body.

All possible and eligible data breaches are to be reported to the Digital ID Regulator and Information Commissioner via DigitalIDRegulator@accc.gov.au.

Key findings and statistics

Below are the findings for the 2024-25 reporting period.

Law enforcement agencies requesting biometric information

There were no requests or requirements made by law enforcement agencies within the relevant reporting period.

Enforcement bodies requesting personal information

The ATO was the only enforcement body identified as having requested or required an accredited entity to disclose personal information (including biometric information) that the accredited entity obtained as part of the provision of the entity's accredited services within the reporting period.

The ATO, in its capacity as an enforcement body, reported a total of 9 requests for personal information for the purposes of enforcement related activities. All 9 requests were complied with in full. In the case of all 9 requests, the ATO had the dual role of serving as both the requesting enforcement body as well as the accredited entity responsible for assessing and discharging requests.[3] A complete list of Digital ID accredited entities can be found on the Australian Consumer & Consumer Commission's website.

Requesting enforcement body	Number of Requests for personal information (including biometric information)	Accredited entity from whom the information was requested
The Australian Taxation Office	9	The Australian Taxation Office

The ATO requested personal information as listed below:

- the individuals' current or former name,
- the individuals' date of birth,
- the individuals' email address, and
- if an individual has Digital ID, the date and time it was created.

In certain cases, the ATO requested access to details about the set up and use of a person's Digital ID, including what documents were used in setting up an individual's myID but not the specific details of the documents. Relevant disclosure requests were processed in accordance with section 54 of the Act.[4]

The limited volume of requests observed is consistent with early expectations for a newly operational regime subject to stringent eligibility criteria and privacy protections. Nonetheless, the reporting architecture established under the Act ensures that use and disclosure of personal and biometric information, including observed increases and decreases in any use and disclosure, will be subject to a clear and enforceable accountability mechanism.

Overall, agencies demonstrated a high degree of engagement and compliance with the statutory reporting requirements in its inaugural year. Notably, a number of agencies have developed

[3] The ATO is accredited to operate the Australian government digital identity services myID and Relationship Authorisation Manager (RAM). MyID is an identity provider used to verify and create a Digital Identity for an individual. RAM is an attribute provider that verifies specific attributes relating to entitlements or characteristics of an individual (for example, enables individuals to be authorised to act on behalf of a business).

[4] ATO in its role as an identity service provider and an accredited service provider is bound by the requirements of *Privacy Act 1988* and the *Digital ID Act 2024*.

internal guidance to support future reporting efforts. Accredited entities complied with all relevant obligations and requests for information. No instances of procedural irregularity, unauthorised access, or non-compliance were identified during this period.

The Government remains committed to maintaining privacy safeguards, including upholding transparency measures under the Act for law enforcement agencies and enforcement bodies.

Key Definitions

Accredited entity

As per section 9 of the Act, each of the following is an accredited entity:

a) an accredited attribute service provider;

b) an accredited identity exchange provider;

c) an accredited identity service provider;

d) if Accreditation Rules are made for the purposes of paragraph 14(1)(d)—an entity that is accredited to provide services of a kind prescribed by the Accreditation Rules for the purposes of that paragraph.

The Accredited Entities Register provides details of Digital ID entities that are, or have been within the previous 12 months, accredited under the Act. The register includes the type of service/s an entity is accredited to provide, the day its accreditation came into force, and any conditions that were imposed on its accreditation.

Accredited entities must comply with the Act and any additional conditions imposed by the Digital ID Regulator or Accreditation Rules. This includes ensuring that accredited services are accessible and inclusive, and that personal information is handled in a secure and compliant manner.

Note: The distinction between an accredited service provider and a relying party and the services each provide. The restrictions on disclosing personal information for enforcement purposes only applies to accredited entities to the extent the accredited entity is providing its accredited service. An accredited service is provided by an accredited entity, while a relying party is an entity that relies on the services of an accredited entity (e.g. for Digital ID for verification purposes). An example of a relying party could be MyGov.

Accredited services

An accredited service refers specifically to the services provided by an accredited entity as part of the verification or authentication process of using a Digital ID. This does not extend to the websites or platforms that the Digital ID enables access to.

As per section 9 of the Act, accredited service, of an accredited entity, means the services provided, or proposed to be provided, by the entity in the entity's capacity as a particular kind of accredited entity.

Law enforcement agency

Under section 4 of the Australian Crime Commission Act 2002, law enforcement agency is defined as:

a) the Australian Federal Police;

b) a Police Force of a State; or

c) any other authority or person responsible for the enforcement of the laws of the Commonwealth or of the States.

Enforcement body

Under section 6 of the *Privacy Act 1988*, enforcement body is defined as:

a) the Australian Federal Police; or

aa) the National Anti - Corruption Commissioner; or

ab) the Inspector of the National Anti - Corruption Commission; or

b) the ACC; or

c) Sport Integrity Australia; or

ca) the Immigration Department; or

d) the Australian Prudential Regulation Authority; or

e) the Australian Securities and Investments Commission; or

ea) the Office of the Director of Public Prosecutions, or a similar body established under a law of a State or Territory; or

f) another agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or

g) another agency, to the extent that it is responsible for administering a law relating to the protection of the public revenue; or

h) a police force or service of a State or a Territory; or

i) the New South Wales Crime Commission; or

j) the Independent Commission Against Corruption of New South Wales; or

k) the Law Enforcement Conduct Commission of New South Wales; or

ka) the Independent Broad - based Anti - corruption Commission of Victoria; or

l) the Crime and Corruption Commission of Queensland; or

la) the Corruption and Crime Commission of Western Australia; or

lb) the Independent Commission Against Corruption of South Australia; or

m) another prescribed authority or body that is established under a law of a State or Territory to conduct criminal investigations or inquiries; or

n) a State or Territory authority, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or

o) a State or Territory authority, to the extent that it is responsible for administering a law relating to the protection of the public revenue.

Contact information

Further information about the reporting obligations under sections 155A and 155B of the Act can be obtained by contacting the Department of Home Affairs:

Criminal Intelligence & Law Enforcement

Department of Home Affairs

3 MOLONGOLO DRIVE

CANBERRA AIRPORT ACT 2609

leps@homeaffairs.gov.au