Identity Verification Services Act 2023

No. 115, 2023

An Act about dealing with information for providing identity verification services, and for related purposes

Note: An electronic version of this Act is available on the Federal Register of Legislation (https://www.legislation.gov.au/)

Contents

Identity Verification Services Act 2023

No. 115, 2023

An Act about dealing with information for providing identity verification services, and for related purposes

[*Assented to 14 December 2023*]

The Parliament of Australia enacts:

Part 1—Preliminary

Division 1—Preliminary

1 Short title

This Act is the *Identity Verification Services Act 2023*.

2 Commencement

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. Sections 1 to 14 and anything in this Act not elsewhere covered by this table	The day after this Act receives the Royal Assent.	15 December 2023
2. Sections 15 to 41	The earlier of: (a) the commencement of rules made under section 44 of this Act; and (b) the start of the day after the end of the period of 6 months beginning on the day this Act receives the Royal Assent.	
3. Section 42	The day after this Act receives the Royal Assent.	15 December 2023
4. Section 43	At the same time as the provisions covered by table item 2.	
5. Section 44	The day after this Act receives the Royal Assent.	15 December 2023

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

(2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

3 Objects of this Act

The objects of this Act are:

(a) to authorise the Department to develop, operate and maintain the 3 approved identity verification facilities (the DVS hub, the Face Matching Service Hub and the NDLFRS); and

(b) to authorise the Department (but not other persons or bodies) to collect, use and disclose identification information communicated to an approved identity verification facility, or generated using the NDLFRS, for purposes relating to:

(i) verifying the identity of an individual using a DVS or FVS; or

(ii) protecting a shielded person or someone else associated with a shielded person using an FVS or FIS; or

(iii) the NDLFRS; and

(c) to protect identification information communicated to approved identity verification facilities, and certain other information relating to the use or security of those facilities, from unauthorised recording, disclosure or access by certain persons who do work for the Department; and

(d) to provide for oversight and scrutiny of the operation and management of the approved identity verification facilities.

Note: The objects in paragraphs 3(a), (b) and (d) are authorised and provided for by Parts 2, 3 and 5. In accordance with the object in paragraph 3(c), Part 4 prohibits the use or disclosure of, or access to, identification information, unless it is in accordance with the objects of this Act or in other limited circumstances.

4 Simplified outline of this Act

The Department may develop and operate the 3 approved identity verification facilities. They are:

(a) the DVS hub, which relays electronic communications between persons and bodies requesting and providing DVSs (which stands for Document Verification Service, a particular kind of 1:1 matching service); and

(b) the Face Matching Service Hub, which relays electronic communications between persons and bodies requesting and providing identity verification services; and

(c) the NDLFRS, which includes a database of identification information from State and Territory authorities and may be used to provide identity verification services.

There are 2 kinds of identity verification services:

(a) 1:1 matching services (FVS (which stands for Face Verification Service) and DVS); and

(b) 1:many matching services (Face Identification Service or FIS).

A 1:1 matching service matches particular biometric information (such as a photograph) or biographic information (such as a name or date of birth) against a particular record. A 1:many matching service compares a facial image (such as a photograph) against other facial images.

The Department may collect identification information through the approved identity verification facilities for any of the following purposes:

(a) providing or developing DVSs or FVSs for the purposes of verifying the identity of individuals;

(b) providing or developing FVSs or FISs for the purposes of protecting identities of persons (or associates) who have legally assumed identities or are under witness protection;

(c) developing, operating or maintaining the NDLFRS.

The Department may use or disclose for any of those purposes information so collected.

An identity verification service involves a request for an electronic comparison of identification information that relates to an individual to do any of the following:

(a) verify the individual's identity;

(b) protect the identity of the individual if the individual is a shielded person;

(c) manage identification information that relates to the individual in the NDLFRS.

Those requests can be made only by parties to agreements that contain safeguards for the privacy of individuals whose identification information is used in requesting or providing the services. The identification information used for comparison with that in the request must have been supplied by a government authority that is party to such an agreement.

Part 4 of this Act prohibits the use or disclosure of, or access to, identification information, unless it is in accordance with the objects of this Act or in other limited circumstances.

Persons who work for the Department, and contractors whose duties relate to an approved identity verification facility, may commit an offence for unauthorised recording, disclosure of or access to certain information held in, generated using or relating to an approved identity verification facility.

Operation and use of the approved identity verification facilities are open to oversight and scrutiny in various ways, including publication of documents, annual assessment by the Information Commissioner and annual reporting.

Division 2—Definitions

Subdivision A—General definitions

5 Definitions

In this Act:

1:1 matching service means DVS or FVS.

1:many matching service means FIS.

access policy has the meaning given by section 14.

approved identity verification facility means:

(a) the DVS hub; or

(b) the Face Matching Service Hub; or

(c) the NDLFRS.

data breach means an occurrence of unauthorised access to, unauthorised disclosure of or loss of identification information.

DVS has the meaning given by section 15.

Note: DVS is short for Document Verification Service, a term used in the intergovernmental agreement.

DVS document means any of the following:

(a) a birth certificate issued by or on behalf of an authority of a State or Territory;

(b) a death certificate issued by or on behalf of an authority of a State or Territory;

(c) a concession card (within the meaning of the *Social Security Act 1991*);

(d) a notice given under section 37 of the *Australian Citizenship Act 2007* stating that a person is an Australian citizen at a particular time;

(e) a certificate issued by an authority of a State or Territory indicating that an individual has changed the individual's name;

(f) a driver's licence (however described) issued by or on behalf of an authority of a State or Territory;

(g) a document issued by or on behalf of an authority of a State or Territory to assist an individual to prove the individual's age or identity;

(h) a document issued to an individual, as a person who is not an Australian citizen, by the Department administered by the Minister administering the *Migration Act 1958* to assist the individual to prove the individual's identity;

(i) a certificate of marriage issued by or on behalf of an authority of a State or Territory whose function it is to register marriages;

(j) a document issued by a court setting out a divorce order made under the *Family Law Act 1975*;

(k) an Australian travel document (within the meaning of the *Australian Passports Act 2005*);

(l) a certificate signed by an officer (within the meaning of the *Migration Act 1958*) stating that, at a specified time, or during a specified period, a specified person was the holder of a visa that was in effect;

(m) an entry in a Roll (within the meaning of the *Commonwealth Electoral Act 1918*) relating to a particular individual;

(n) an aviation security identification card issued under regulations made for the purposes of the *Aviation Transport Security Act 2004*;

(o) an MSIC issued under regulations made for the purposes of the *Maritime Transport and Offshore Facilities Security Act 2003*;

(p) a medicare card (within the meaning of subsection 84(1) of the *National Health Act 1953*).

DVS hub means a facility that:

(a) is for relaying electronic communications between persons and bodies for the purposes of requesting and providing DVSs; and

(b) is developed, operated and maintained by the Department under Part 2.

DVS information has the meaning given by section 6.

electronic communication means a communication of information, in the form of data, text or images by means of guided electromagnetic energy, unguided electromagnetic energy or both, carried by a telegraphic, telephonic or other like service within the meaning of section 51(v) of the Constitution.

entrusted person has the meaning given by section 30.

Face Matching Service Hub means a facility that:

(a) is for relaying electronic communications between persons and bodies for the purposes of requesting and providing identity verification services; and

(b) is developed, operated and maintained by the Department under Part 2.

face-matching service information has the meaning given by section 6.

facial image means a digital still image of an individual's face (whether or not including the shoulders).

FIS has the meaning given by section 16.

Note: FIS is short for Face Identification Service, a term used in the intergovernmental agreement.

FVS has the meaning given by section 19.

Note: FVS is short for Face Verification Service, a term used in the intergovernmental agreement.

government authority means:

(a) an authority of the Commonwealth; or

(b) an authority of a State or Territory;

other than a local government authority.

government identification document means a document or other thing that:

(a) contains identification information; and

(b) can be used to identify an individual or to pass an individual off as someone else (whether living, dead, real or fictitious); and

(c) is issued by or on behalf of a government authority.

identification information has the meaning given by section 6.

identity verification service means:

(a) a 1:1 matching service; or

(b) a 1:many matching service.

intergovernmental agreement means the Intergovernmental Agreement on Identity Matching Services made on 5 October 2017 by the Commonwealth, the States, the Australian Capital Territory and the Northern Territory.

Note: The intergovernmental agreement must be published on the Department's website (see section 39).

NDLFRS means a system that consists of:

(a) a database of identification information that:

(i) is also either contained in government identification documents issued by or on behalf of an authority of a State or Territory or associated with those documents by the authority; and

(ii) is supplied by or on behalf of the authority to the Department by electronic communication for inclusion in the database; and

(b) a system for biometric comparison of facial images with facial images that are in the database described in paragraph (a);

and is developed, operated and maintained by the Department under Part 2.

Note: NDLFRS is short for National Driver Licence Facial Recognition Solution, a term used in the intergovernmental agreement.

NDLFRS hosting agreement has the meaning given by section 13.

non-government entity means a person, or body, other than:

(a) the Commonwealth, a State or a Territory; or

(b) a government authority.

Note: Local government authorities are non-government entities because they are excluded from the definition of ***government authority***. Authorities of New Zealand are non-government entities because they are not covered by the definition of ***government authority***.

participation agreement has the meaning given by section 8.

personal information has the meaning given by section 6 of the *Privacy Act 1988*.

privacy impact assessment has the meaning given by subsection 33D(3) of the *Privacy Act 1988*.

protected information has the meaning given by section 30.

rules means rules made under section 44.

Secretary means the Secretary of the Department.

shielded person means a person to whom one or more of the following paragraphs apply:

(a) the person has acquired or used an assumed identity under Part IAC of the *Crimes Act 1914* or a corresponding assumed identity law within the meaning of that Part;

(b) an authority for the person to acquire or use an assumed identity has been granted under that Part or such a law;

(c) a witness identity protection certificate has been given for the person under Part IACA of the *Crimes Act 1914*;

(d) a corresponding witness identity protection certificate has been given for the person under a corresponding witness identity protection law within the meaning of Part IACA of the *Crimes Act 1914*;

(e) the person is a participant (as defined in the *Witness Protection Act 1994*);

(f) the person is or was on a witness protection program conducted by a State or Territory in which a complementary witness protection law (as defined in the *Witness Protection Act 1994*) is in force;

(g) the person is involved in administering such a program under such a law and the person has acquired an identity under that law.

6 Definitions relating to identification information

*Definition of **identification information***

(1) ***Identification information*** is:

(a) face-matching service information; or

(b) DVS information.

*Definition of **face-matching service information***

(2) ***Face-matching service information*** that relates to an individual (whether living, dead, real or fictitious) is any of the following, subject to subsections (4) and (5):

(a) a name by which the individual is or has been known;

(b) a current or former address of the individual;

(c) the place or date the individual was born;

(d) the age of the individual (whether expressed by reference to a range or not);

(e) the current or former sex, gender identity or intersex status of the individual;

(f) information about whether the individual is alive or dead;

(g) any information that is:

(i) contained in a driver's licence (however described) issued by or on behalf of an authority of a State or Territory in a name of the individual; or

(ii) otherwise associated with such a licence by such an authority;

(h) any information that is:

(i) contained in any document (however described) that is issued by or on behalf of an authority of a State or Territory in a name of the individual, contains a photograph purporting to be of the individual and can be used to assist in proving the individual's identity; or

(ii) otherwise associated with such a document by the authority;

(i) any information that is:

(i) contained in a document issued to the individual, as a person who is not an Australian citizen, by the Department administered by the Minister administering the *Migration Act 1958* to assist the individual to prove the individual's identity; or

(ii) otherwise associated with such a document by that Department;

(j) any information that is:

(i) contained in an Australian travel document (within the meaning of the *Australian Passports Act 2005*) issued in a name of the individual; or

(ii) otherwise associated with the Australian travel document by the Minister administering the *Australian Passports Act 2005* or the Department administered by that Minister; or

(iii) otherwise associated with the Australian travel document by a government authority by which the travel document may be inspected or seized under a law of the Commonwealth or of a State or Territory;

(k) any information that is:

(i) contained in a foreign travel document (within the meaning of the *Foreign Passports (Law Enforcement and Security) Act 2005*) issued in a name of the individual; or

(ii) otherwise associated with the foreign travel document by a government authority by which the travel document may be inspected or seized under a law of the Commonwealth or of a State or Territory;

(l) the individual's current or former citizenship;

(m) any information that is:

(i) contained in a current or past application for Australian citizenship for the individual; or

(ii) contained in a document issued by an authority of the Commonwealth to provide evidence that the individual is or was an Australian citizen; or

(iii) otherwise associated with an application or document described in subparagraph (i) or (ii) by the Department administered by the Minister administering the *Australian Citizenship Act 2007*;

(n) information about a visa, or an entry permit under the *Migration Act 1958*, that the individual holds or held;

(o) any information that is:

(i) contained in a current or past application for a visa, or entry permit, for the individual under the *Migration Act 1958*; or

(ii) contained in a visa, or entry permit, for the individual granted under that Act; or

(iii) otherwise associated with an application, visa or entry permit described in subparagraph (i) or (ii) by the Department administered by the Minister administering that Act;

(p) a facial image of the individual, a biometric template derived from such an image or a result of biometric comparison involving such an image;

(q) information about the outcome of a comparison involved in an FVS requested in relation to the individual.

*Definition of **DVS information***

(3) ***DVS information*** that relates to an individual is either of the following, subject to subsections (4) and (5):

(a) information (but not a facial image or biometric information) that either:

(i) is contained in a document (the ***specimen document***) that relates to the individual and purports to be a DVS document of a particular kind; or

(ii) is, or is reasonably expected to be, associated, with a DVS document of a particular kind relating to the individual, by a government authority that is responsible for the issue of DVS documents of that kind;

and helps indicate whether the specimen document is a DVS document of that kind;

(b) information about the outcome of a comparison involved in a DVS relating to the individual.

What is not face-matching service information or DVS information

(4) The following is neither face-matching service information, nor DVS information, that relates to an individual:

(a) information or an opinion that relates to the individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation or practices; or

(ix) criminal record;

(b) health information (within the meaning of the *Privacy Act 1988*) that relates to the individual;

(c) genetic information that relates to the individual.

(5) Subsection (4) does not prevent information described in any of the paragraphs of subsection (2) or (3) from being face-matching service information or DVS information if the information is not primarily of any of the kinds described in subsection (4), even if information of any of those kinds can reasonably be inferred from the information.

Example 1: Even if an individual's racial or ethnic origin can reasonably be inferred from the individual's name or place of birth, this does not prevent the individual's name or place of birth from being face-matching service information or DVS information.

Example 2: Even if an individual's racial or ethnic origin or religious affiliations can reasonably be inferred from a facial image of the individual, this does not prevent the image from being face-matching service information.

Identification information taken to be personal information

(6) Identification information is taken to be personal information for the purposes of the *Privacy Act 1988*.

Subdivision B—Common provisions for definitions of identity verification services

7 Simplified outline of this Subdivision

Two types of agreement govern the requesting and provision of identity verification services:

(a) participation agreements (which are agreements between the Department and other authorities, persons and bodies about the requesting and provision of identity verification services using the approved identity verification facilities); and

(b) the NDLFRS hosting agreement (which is an agreement between the Department and authorities of a State or Territory that supply identification information stored and used in the NDLFRS).

A request for an identity verification service can be made only by a party to a participation agreement, and only identification information made available by a party to a participation agreement can be used in an identity verification service.

The Department may develop, operate and maintain the approved identity verification facilities. The Department is required to maintain the security of electronic communications to and from the facility, including by encrypting the information, and to protect the information from unauthorised interference or unauthorised access.

Participation agreements and the NDLFRS hosting agreement contain safeguards for the privacy of individuals whose identification information is used in requesting identity verification services or responding to such requests. The safeguards include committing the parties to the agreement to complying with

standards set by the *Privacy Act 1988* or similar State or Territory laws (even if those standards would not otherwise apply to a party).

Participation agreements also need to provide for a range of other privacy safeguards relating to identity verification services, including:

(a) privacy impact assessments of requesting the services; and

(b) obtaining an individual's express consent to the collection, use and disclosure of the individual's identification information for the purposes of requesting the services (unless the collection, use and disclosure is by a government authority authorised by another law to do so); and

(c) limits on the purposes for which the services may be requested and on what may be done with information received in response to requests; and

(d) annual reporting and auditing of compliance with agreements; and

(e) suspension or termination of a party's ability to request services if the party has not complied with the agreement or access policies for the services.

8 Definition of *participation agreement*

(1) A ***participation agreement*** is a written agreement, between the Department (representing the Commonwealth) and one or more other parties, that:

(a) deals with the requesting and provision of identity verification services of one or more kinds using identification information made available by the parties; and

(b) meets the requirements in sections 9, 10, 11 and 12.

Timing and nature of agreement

(2) To avoid doubt:

(a) an agreement may be a participation agreement whether it was made before, on or after the commencement of this section; and

(b) different participation agreements may be made between the Department and different other parties; and

(c) paragraph (1)(b) and sections 9, 10, 11 and 12 do not limit the matters a participation agreement may deal with.

9 General privacy obligations of parties to participation agreement

(1) Each party to a participation agreement must:

(a) be subject to the *Privacy Act 1988*; or

(b) be subject to a privacy law that:

(i) is a law of a State or Territory; and

(ii) is prescribed by the rules for the purposes of this subparagraph; or

(c) agree in the agreement to comply with the Australian Privacy Principles, with any modifications of subclauses 7.8 and 12.2 of those principles (about laws of the Commonwealth) specified in the agreement, as if the party were an APP entity; or

(d) be a government authority prescribed by the rules for the purposes of this paragraph; or

(e) if the agreement deals only with the requesting of DVSs by, and provision of DVSs to, an authority of New Zealand or a person or body operating in New Zealand—be an authority, person or body subject to the *Privacy Act 1993* of New Zealand.

Note: A DVS is the only identity verification service available to a party to an agreement described in paragraph (e).

(2) A participation agreement must provide for:

(a) privacy impact assessments of requesting identity verification services; and

(b) the obtaining of an individual's express consent to the collection, use and disclosure, for the purposes of requesting identity verification services, of identification information

that relates to the individual included in such a request, unless:

(i) the request is made by or on behalf of a government authority; and

(ii) collection, use and disclosure of that information for the purposes of protecting a shielded person, or someone else associated with a shielded person, are implicit in functions conferred by law on the authority; and

(c) the provision, to an individual from whom such express consent is being sought, of information about matters described in subsection (3); and

(d) each party to have arrangements for dealing with complaints by individuals whose identification information is held by the party; and

(e) each party to the agreement (except the Department) to report to the Department on breaches of security that relate to the party and are relevant to a matter dealt with in the agreement; and

(f) the Department to inform the Information Commissioner of a breach of security that:

(i) is reported to the Department under a provision of the agreement covered by paragraph (e); and

(ii) is a data breach that is reasonably likely to result in serious harm to an individual whose identification information is involved in the breach; and

(g) the Department to notify each party to the agreement that is relevant to, or impacted by, a data breach of which the Information Commissioner is informed under paragraph (f); and

(h) each party notified under paragraph (g) of a data breach, that is impacted by that breach, to take reasonable steps to notify each individual to whom the identification information relates.

(3) For the purposes of paragraph (2)(c), the matters are as follows:

(a) how the party seeking express consent uses identity verification services;

(b) how any facial images of the individual collected by the party from the individual for requesting an identity verification service or from a response to a request for an identity verification service will be used and disposed of;

(c) whether any such facial images will be retained or used for purposes other than those for which the identity verification service is to be requested;

(d) what legal obligations the party seeking to collect the identification information has in relation to that collection;

(e) what rights the individual has in relation to the collection of the identification information;

(f) the consequences of the individual declining to consent;

(g) where the individual can get information about making complaints relating to the collection, use and disclosure of the identification information for the purposes of requesting and provision of identity verification services;

(h) where the individual can get information about the operation and management of the approved identity verification facilities by the Department in connection with the requesting and provision of identity verification services.

(4) A participation agreement must provide that a party to the agreement is not authorised to use or disclose identification information obtained for the purposes of requesting or providing identity verification services for the purposes of any of the following:

(a) engaging in activities that would allow the party to create a data profile of the person whose identity is being verified (including where it would allow the person's behaviour to be tracked (whether or not online));

(b) offering to supply goods or services;

(c) advertising or promoting goods or services;

(d) enabling another person or entity to offer to supply goods or services;

(e) enabling another person or entity to advertise or promote goods or services;

(f) market research.

10 Extra privacy obligations of parties to participation agreement that request services

(1) A participation agreement must require each party to the agreement that proposes to request identity verification services:

(a) either:

(i) to request a DVS or FVS for the purposes of verifying the identity of an individual; or

(ii) to request an FVS or FIS for the purposes of protecting a shielded person or someone else associated with such a person; and

(b) to comply with the access policy for each service the party requests; and

(c) not to use the outcome of an identity verification service the party requested in relation to an individual as the only evidence of the individual's identity in criminal or civil proceedings to which the individual is a party.

(2) A participation agreement must provide for each party to the agreement that proposes to request identity verification services:

(a) not to disclose identification information received by the party as a result of an identity verification service the party requested, except:

(i) as required by law; or

(ii) as permitted by law in circumstances specified in, or identified in accordance with, the agreement; and

(aa) if the identity verification service is an FVS—to take reasonable steps to destroy each facial image of an individual that is created, for the purposes of the request, by the party requesting the service, as soon as reasonably practicable after the image is no longer required for the purposes of the request, unless the image is:

(i) a Commonwealth record (within the meaning of the *Archives Act 1983*); or

(ii) required by a law of the Commonwealth, a State or a Territory, or by an order of a court or tribunal, to be retained; and

(b) if the party is a government authority—not to permit an individual who is an officer, member of staff, employee or contractor of the party to:

(i) make on behalf of the authority a request for an identity verification service that may result in a facial image being provided in response; or

(ii) deal with a facial image provided in response to such a request;

unless the individual has been trained in facial recognition and image comparison.

Note: Facial images are not provided in response to requests by or on behalf of non-government entities.

10A Failure to comply with participation agreements

(1) This section applies if:

(a) a party to a participation agreement is subject to the *Privacy Act 1988*; and

(b) an act or practice of the party, relating to personal information about an individual, does not comply with a requirement of:

(i) the agreement in relation to a matter covered by section 9 or 10 (other than paragraph 10(1)(b)) of this Act; or

(ii) rules prescribed for the purposes of subsection 44(1A) of this Act.

(2) For the purposes of the *Privacy Act 1988*, the act or practice is taken to be:

(a) an interference with the privacy of the individual; and

(b) covered by sections 13 and 13G of that Act.

11 Participation agreement must let parties limit use of identification information they make available for identity verification services

A participation agreement must provide for a party that is a government authority that makes available identification

information for an identity verification service (except in a request for the service) to be able to limit the use of that information.

12 Requirements relating to compliance with participation agreement

A participation agreement must provide for:

(a) annual auditing of compliance with the agreement; and

(b) each party to the agreement (except the Department) to report annually to the Department on the party's compliance with the agreement; and

(c) suspension or termination of the ability of a party to the agreement to request identity verification services if the party does not comply with the agreement, rules made for the purposes of subsection 44(1A), or access policies for those services.

Note: Under subsection 44(1A), the rules may prescribe requirements relating to privacy with which a party to a participation agreement must comply.

13 NDLFRS hosting agreement

(1) The ***NDLFRS hosting agreement*** is a written agreement that:

(a) is between the Department (representing the Commonwealth) and each authority that:

(i) is an authority of a State or Territory; and

(ii) meets the requirement in subsection (2); and

(iii) supplies or proposes to supply identification information to the Department for inclusion in a database in the NDLFRS; and

(b) deals with the NDLFRS and the collection, use and disclosure of identification information in a database in the NDLFRS; and

(c) meets the requirements in subsections (3), (4) and (5).

State and Territory parties must be subject to privacy obligations

(2) Each authority of a State or Territory that is party to the agreement must:

(a) be subject to a privacy law that:
  (i) is a law of the State or Territory; and
  (ii) is prescribed by the rules for the purposes of this subparagraph; or
(b) be one of the following to which the *Privacy Act 1988* applies (with or without modifications) as if it were an organisation:
  (i) a State or Territory authority (as defined in that Act);
  (ii) an instrumentality of a State or Territory; or
(c) agree in the agreement to comply with the Australian Privacy Principles, with any modifications of subclauses 7.8 and 12.2 of those principles (about laws of the Commonwealth) specified in the agreement, as if the party were an APP entity.

Note: The Department, which is the other party to the agreement, is subject to the *Privacy Act 1988*.

Requirements on each State or Territory party

(3) The agreement must provide for each party that is an authority of a State or Territory:
(a) to take reasonable steps to inform each individual whose identification information is, or is to be, included in a database in the NDLFRS of that inclusion; and
(b) to provide each individual whose identification information is included in a database in the NDLFRS with means of:
  (i) finding out what that information is; and
  (ii) having any errors in that information corrected in the database; and
(c) to inform each such individual and the Department of any data breaches that:
  (i) involve identification information that relates to the individual and the NDLFRS; and
  (ii) are reasonably likely to result in serious harm to the individual; and
(d) to provide means for dealing with complaints by individuals relating to the NDLFRS and identification information that

relates to them that is included in a database in the NDLFRS; and

(e) to report annually to the Department on the party's compliance with the agreement.

Requirements on the Department

(4) The agreement must provide for the Department:

(a) to maintain the security of identification information included in a database in the NDLFRS, including by encrypting the information; and

(b) to inform the other parties to the agreement of any data breaches involving that information and the NDLFRS; and

(c) to inform the Information Commissioner of any data breaches that:

(i) involve that information and the NDLFRS; and

(ii) are reasonably likely to result in serious harm to an individual to whom that information relates.

Note: For paragraph (4)(a), see also paragraph 25(a).

Requirement relating to compliance

(5) The agreement must provide for suspension or termination of the ability of a party to the agreement to request identity verification services involving the NDLFRS if the party does not comply with the agreement.

Timing and nature of agreement

(6) To avoid doubt:

(a) an agreement may be the NDLFRS hosting agreement whether it was made before, on or after the commencement of this section; and

(b) paragraph (1)(c) and subsections (3), (4) and (5) do not limit the matters the agreement may deal with.

14 Access policies for services

The ***access policy*** for a service is the conditions that:

(a) are to be complied with by parties to participation agreements for the parties to have access (on request by the parties) to services of that kind; and

(b) are set out in a document approved by the Coordination Group provided for by the intergovernmental agreement; and

(c) include conditions providing for the parties to give the Secretary statements of the legal basis for disclosing and using identification information for the purposes of requesting and providing services of that kind to the parties.

Note: Under section 39, the Secretary must publish documents setting out access policies.

Subdivision C—Definition of DVS

15 Definition of *DVS*

(1) A service is a ***DVS*** if:

(a) it is, or is sought to be, provided on a request made by or on behalf of an authority, person or body (each the ***requesting party***); and

(b) the requesting party is a party to a participation agreement; and

(c) the request includes DVS information, that relates to an individual (other than information described in paragraph 6(3)(b)), and to a specimen document purporting to be a DVS document that:

(i) is of a kind specified in the request; and

(ii) is issued by a government authority that is or was responsible for the issue of DVS documents of that kind; and

(d) the service involves, or is to involve, an electronic comparison of the DVS information described in paragraph (c) and information that:

(i) is contained in DVS documents of the kind specified in the request, or is associated with such documents by the government authority (the ***issuing authority***) that is responsible for issuing them and is a party to a participation agreement; and

(ii) is made available for the comparison by the issuing authority; and

(e) the comparison is carried out in accordance with any limitations, provided for under that participation agreement, subject to which the issuing authority made the information available for the comparison; and

(f) the purpose of the comparison is to help determine whether the specimen document is a DVS document of the kind identified in the request; and

(g) the response to the requesting party about the outcome of the comparison is limited to either:

(i) a statement that the information compared matched; or

(ii) a statement that the information compared did not match, with or without reasons why the information did not match; and

(h) the request and the response to the request are communicated by electronic communications relayed through the DVS hub or the Face Matching Service Hub.

Note 1: DVS is short for Document Verification Service, a term used in the intergovernmental agreement.

Note 2: DVS is an example of a 1:1 matching service (see the definition of ***1:1 matching service*** in section 5).

(2) The following provisions do not apply in relation to a service requested within the period specified by subsection (3) after the commencement of this section:

(a) paragraph (1)(b);

(b) subparagraph (1)(d)(i), so far as it relates to the issuing authority being a party to a participation agreement;

(c) paragraph (1)(e).

(3) For the purposes of subsection (2), the period is:

(a) 12 months; or

(b) if the rules prescribe a longer period of up to 18 months for the purposes of this paragraph—that longer period.

Subdivision D—Definition of FIS

16 Definition of *FIS*

A service is an ***FIS*** if:

(a) it is, or is sought to be, provided on a request; and

(b) the requirements in section 17 are met in relation to the request; and

(c) the service involves, or is to involve, a comparison that has the characteristics and purpose set out in section 18; and

(d) the request and the outcome of the comparison are communicated by electronic communications relayed through the Face Matching Service Hub.

Note 1: FIS is short for Face Identification Service, a term used in the intergovernmental agreement.

Note 2: FIS is the only kind of 1:many matching service that is permitted under this Act.

17 Requirements for valid request for FIS

Requesting authorities

(1) A request for an FIS must be made only:

(a) by any of the following officers of a Commonwealth, State or Territory government authority that is a party to a participation agreement:

(i) a law enforcement officer or intelligence officer (within the meaning of section 15K of the *Crimes Act 1914*);

(ii) an officer (however described) of an agency authorised under a corresponding assumed identity law (within the meaning of section 15K of the *Crimes Act 1914*);

(iii) an officer (however described) of an approved authority (within the meaning of the *Witness Protection Act 1994*) that is permitted to participate in the National Witness Protection Program under that Act, or a complementary witness protection law declared under section 3AA of that Act; and

(b) if the officer is required to make the request for the purpose of protecting the identity of a shielded person or someone else associated with a shielded person.

Person making request

(2) The person making the request on behalf of the authority must be an officer who is approved as a suitable person to make the request (or requests of that kind) by:

(a) the head (however described) of the authority; or

(b) a person who:

(i) is the holder of a management office or position in the authority; and

(ii) is authorised, by notice in writing given to the Department, by that head to approve persons to make requests for FISs on behalf of the authority; and

(iii) is senior to the person making the request.

Note: To comply with the participation agreement to which the authority is party, an officer approved to make the request must have been trained in facial recognition and image comparison: see paragraph 10(2)(b).

Request stating relevant activity

(3) The request must:

(a) include a single facial image of an individual (whether or not other face-matching service information that relates to the individual is included); and

(b) specify the kinds of government identification documents against which the face-matching service information in the request is to be compared, partly by reference to whether the authority by or on behalf of which the documents are issued is:

(i) an authority of the Commonwealth; or

(ii) an authority of a specified State; or

(iii) an authority of a specified Territory.

Note: Making a false or misleading statement in the request may be an offence against section 136.1 of the *Criminal Code*.

Endorsement of request

(4) The request must be:

(a) endorsed by the head (however described) of the authority, or a person who:

(i) is the holder of a management office or position in the authority; and

(ii) is authorised, by notice in writing given to the Department, by that head to endorse requests for FISs made on behalf of the authority; and

(iii) is senior to the person making the request; and

(b) made by electronic communication to the Face Matching Service Hub.

Note: The endorsement may be given at the same time as, or after, the request is made by electronic communication to the Face Matching Service Hub.

(5) A person must not endorse a request made on behalf of an authority unless the person is satisfied that the request is made for the purposes of:

(a) protecting the shielded person, or associate, stated in the request; and

(b) the performance of the authority's functions.

18 Characteristics and purpose of comparison involved in FIS

(1) The comparison involved in an FIS is an electronic comparison of:

(a) a single facial image of an individual, and other face-matching service information (if any) that relates to the individual, that is included in the request for the service; and

(b) face-matching service information that:

(i) relates to one or more individuals; and

(ii) is contained in, or associated with, one or more government identification documents of one or more kinds specified in the request; and

(iii) is made available for the comparison by a government authority (the ***supplying authority***) that is a party to a participation agreement.

(2) The comparison is carried out in accordance with any limitations, provided for under the participation agreement, subject to which the supplying authority made the face-matching service information available for the comparison.

(3) The comparison is for the purpose of protecting an individual who is a shielded person, or someone else associated with a shielded person.

Subdivision E—Definition of FVS

19 Definition of *FVS*

A service is an ***FVS*** if:

(a) it is, or is sought to be, provided on a request, made by or on behalf of a party (the ***requesting party***) to a participation agreement that does not deal only with the requesting of DVSs by, and provision of DVSs to, an authority of New Zealand or a person or body operating in New Zealand; and

(b) the request includes face-matching service information that relates to the individual; and

(c) the service involves, or is to involve, a comparison that has the characteristics and purpose set out in section 20; and

(d) if the requesting party is a non-government entity—the response to the requesting party about the outcome of the comparison:

(i) is either that the comparison resulted in a match for the individual or that the comparison did not result in a match for the individual; and

(ii) does not contain any other face-matching service information that relates to the individual; and

(e) the request and the response are communicated by electronic communications relayed through the Face Matching Service Hub.

Note 1: FVS is short for Face Verification Service, a term used in the intergovernmental agreement.

Note 2: FVS is an example of a 1:1 matching service (see the definition of ***1:1 matching service*** in section 5).

20 Characteristics and purpose of comparison involved in FVS

(1) The comparison involved in an FVS is an electronic comparison of:

(a) face-matching service information that relates to the individual that is included in the request for the service; and

(b) face-matching service information that:

(i) is contained in, or associated with, a government identification document of a kind specified in the request that was issued to the individual; and

(ii) is made available for the comparison by a government authority (the ***supplying authority***) that is a party to a participation agreement.

(2) The comparison is carried out in accordance with any limitations, provided for under the participation agreement, subject to which the supplying authority made the face-matching service information available for the comparison.

(3) The comparison is for the purpose of:

(a) verifying the identity of the individual; or

(b) protecting an individual who is a shielded person, or someone else associated with a shielded person.

Division 3—Miscellaneous

21 False and misleading statements in requests for services

To avoid doubt, a request for an identity verification service is an application for a benefit for the purposes of section 136.1 of the *Criminal Code*.

Note: That section creates offences for making false or misleading statements in applications for benefits.

22 This Act binds Crown

This Act binds the Crown in each of its capacities.

Part 2—Developing, operating and maintaining approved identity verification facilities

23 Simplified outline of this Part

In accordance with the object of this Act covered by paragraph 3(a), the Department may develop, operate and maintain the 3 approved identity verification facilities (the DVS hub, the Face Matching Service Hub and the NDLFRS).

The Department is required to maintain the security of electronic communications to and from the facility, including by encrypting the information, and to protect the information from unauthorised interference or unauthorised access.

24 Department may develop, operate and maintain approved identity verification facilities

(1) The Department may develop, operate and maintain the approved identity verification facilities.

(2) The authorisation by subsection (1) to develop, operate and maintain the DVS hub does not limit the authorisation by that subsection to develop, operate and maintain the Face Matching Service Hub.

25 How facilities are to be developed, operated and maintained

In developing, operating and maintaining an approved identity verification facility, the Department must:

(a) maintain the security of electronic communications to and from the facility, including by encrypting the information; and

(b) protect the information from unauthorised interference or unauthorised access.

Part 3—Authorising collection, use and disclosure of identification information

Division 1—Simplified outline

26 Simplified outline of this Part

In accordance with the object of this Act covered by paragraph 3(b), the Department may collect certain identification information by means of particular approved identity verification facilities for any of the following purposes:

(a) providing or developing DVSs or FVSs for the purposes of verifying the identity of individuals;

(b) providing or developing FVSs or FISs for the purposes of protecting identities of persons (or associates) who have legally assumed identities or are under witness protection;

(c) developing, operating or maintaining the NDLFRS.

The Department may use or disclose for any of those purposes:

(a) information so collected (regardless of the purpose for which it was collected); and

(b) identification information generated by the NDLFRS.

Division 2—Collection, use and disclosure of identification information by the Department

27 Collection of identification information by the Department

General

(1) The Department may collect identification information (whether or not it is sensitive information as defined in the *Privacy Act 1988*) that relates to an individual from someone other than the individual, if the collection:

(a) is for a purpose described in subsection (2); and

(b) is covered by subsection (3), (4) or (5).

Note: One effect of this section is that such collection of identification information is authorised for the purposes of provisions of Australian Privacy Principle 3, such as paragraph 3.4(a) (about sensitive information) and subparagraph 3.6(a)(ii) (about personal information).

Purpose of collection

(2) The purposes for which identification information may be collected under this section (or used or disclosed under section 28) are as follows:

(a) providing a DVS and FVS for the purpose of verifying the identity of a person;

(b) providing an FVS or FIS for the purpose of protecting a shielded person or someone else associated with such a person;

(c) developing identity verification services, or facilities for providing those services, for the purpose mentioned in paragraph (a) or (b) (as applicable);

(d) developing, operating or maintaining the NDLFRS.

Collection of DVS information via DVS hub

(3) This subsection covers collection of DVS information by means of an electronic communication to the DVS hub requesting provision of a DVS or responding to a request for provision of a DVS.

Collection of identification information via Face Matching Service Hub

(4) This subsection covers collection of identification information by means of an electronic communication to the Face Matching Service Hub that:
  (a) requests provision of an identity verification service; or
  (b) responds to a request for provision of an identity verification service; or
  (c) supplies the information to a database in the NDLFRS.

Collection of identification information via NDLFRS

(5) This subsection covers collection of identification information by means of an electronic communication to the NDLFRS that:
  (a) requests provision of an identity verification service; or
  (b) supplies the information to a database in the NDLFRS.

This section does not authorise disclosure to the Department

(6) This section does not, by implication:
  (a) authorise the disclosure of identification information to the Department; or
  (b) affect whether another provision of a law of the Commonwealth or of a State or Territory providing for collection of information authorises (by implication) disclosure of that information to the person or body authorised by that provision to collect it.

28 Use and disclosure of identification information by the Department

(1) The Department may, for any purpose described in subsection 27(2), use or disclose identification information:
  (a) collected by means of an electronic communication to an approved identity verification facility; or
  (b) held in, or generated using, the NDLFRS.

Note: One effect of this section is that such use or disclosure of identification information by the Department is authorised for the

purposes of provisions of Australian Privacy Principle 6, such as paragraph 6.2(b) (use or disclosure of personal information authorised by law).

(2) This section does not, by implication:

(a) authorise a person or body to collect identification information disclosed by the Department under subsection (1); or

(b) affect whether another provision of a law of the Commonwealth or of a State or Territory providing for disclosure of information authorises (by implication) collection of that information by a person or body to which the information is disclosed under that provision.

Part 4—Protection of information

Division 1—Simplified outline

29 Simplified outline of this Part

An object of this Act is to protect identification information communicated to approved identity verification facilities, and certain other information relating to the use or security of those facilities.

This Act does this by prohibiting the use or disclosure of, or access to, identification information, unless it is in accordance with the objects of this Act or in other limited circumstances.

Current and former entrusted persons may commit an offence if they record, disclose or access certain information connected with an approved identity verification facility.

Basically, entrusted persons are the following:

(a) persons who work for the Department;

(b) contractors (and their officers and employees) engaged to provide services to the Department in connection with an approved identity verification facility.

There are exceptions for recording, disclosure or access authorised by a law of the Commonwealth or of a State or Territory. The exceptions include recording, disclosure or access:

(a) for the purposes of this Act; or

(b) in exercising powers, or performing functions or duties, relating to an approved identity verification facility; or

(c) for lessening or preventing a serious and imminent threat to human life or health; or

(d) relating to the work of an official of an integrity agency; or

(e) with the express consent of the person to whom the information recorded, disclosed or accessed relates.

Division 2—Prohibition on recording or disclosure of, or access to, information by entrusted persons

30 Prohibition on recording or disclosure of, or access to, information by entrusted persons

Offence for recording or disclosing information

(1) A person commits an offence if:
  (a) the person is, or has been, an entrusted person; and
  (b) the person has obtained protected information in the person's capacity as an entrusted person; and
  (c) the person:
    (i) makes a record of the information; or
    (ii) discloses the information to another person.

Note: The fault element for the physical elements in paragraphs (a) and (b) is recklessness: see section 5.6 of the *Criminal Code*.

Penalty: Imprisonment for 2 years.

Offence for accessing information

(2) A person commits an offence if:
  (a) the person is an entrusted person; and
  (b) the person accesses protected information.

Note: The fault element for the physical elements in paragraph (a) is recklessness: see section 5.6 of the *Criminal Code*.

Penalty: Imprisonment for 2 years.

Exceptions

(3) Each of the following is an exception to the prohibition in subsection (1) or (2):
  (a) the conduct is authorised by a law of the Commonwealth or of a State or Territory;

(b) the conduct is in compliance with a requirement under a law of the Commonwealth or of a State or Territory.

Note 1: A defendant bears an evidential burden in relation to the matter in subsection (3): see subsection 13.3(3) of the *Criminal Code*.

Note 2: For paragraph (3)(a), see also sections 31 to 35 which authorise conduct.

*Definitions of **entrusted person** and **protected information***

(4) In this Act:

entrusted person means:

(a) the Secretary; or

(b) an APS employee in the Department; or

(c) a person who is:

(i) an employee of an Agency (within the meaning of the *Public Service Act 1999*); or

(ii) an officer or employee of a State or Territory; or

(iii) an officer or employee of a government authority; or

(iv) an officer or employee of the government of a foreign country; or

(v) an officer or employee of an authority of a foreign country; or

(vi) an officer or employee of a public international organisation (within the meaning of section 70.1 of the *Criminal Code*);

and whose services are made available to the Department; or

(d) a contractor engaged to provide services to the Department in connection with an approved identity verification facility (whether the contractor is engaged directly by the Commonwealth or as a subcontractor); or

(e) an officer or employee of such a contractor whose duties relate wholly or partly to an approved identity verification facility.

protected information means any of the following:

(a) identification information that was obtained by a person, in the person's capacity as an entrusted person, from:

(i) an electronic communication to or from an approved identity verification facility; or

(ii) the NDLFRS;

(b) information about either of the following:

(i) the making, content or addressing of an electronic communication made to or from an approved identity verification facility;

(ii) identification information relating to a particular individual held in, or generated using, the NDLFRS;

that was obtained by a person, in the person's capacity as an entrusted person;

(c) information that enables access to an approved identity verification facility and was obtained by a person, in the person's capacity as an entrusted person.

31 Exercising powers, or performing functions or duties, as an entrusted person

An entrusted person may make a record of, disclose or access protected information if the record is made, or the information is disclosed or accessed:

(a) for the purposes of this Act; or

(b) in the course of exercising powers, or performing functions or duties, relating wholly or partly to an approved identity verification facility.

32 Disclosure to lessen or prevent threat to life or health

(1) An entrusted person may disclose protected information if:

(a) the entrusted person reasonably believes that the disclosure is necessary to lessen or prevent a serious and imminent threat to the life or health of an individual; and

(b) the disclosure is for the purpose of lessening or preventing that threat.

(2) An entrusted person may make a record of or access protected information for the purpose of disclosing the protected information under subsection (1).

33 Information communicated etc. to integrity agencies

(1) An entrusted person may disclose protected information if:

(a) the disclosure is to any of the following persons:

(i) the Inspector-General of Intelligence and Security, or a person covered by subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*;

(ii) the Commonwealth Ombudsman, or another officer (within the meaning of subsection 35(1) of the *Ombudsman Act 1976*);

(iii) the Information Commissioner, a member of the staff of the Office of the Information Commissioner, or a consultant engaged under the *Australian Information Commissioner Act 2010*;

(iv) the National Anti-Corruption Commissioner, or another staff member of the NACC (within the meaning of the *National Anti-Corruption Commission Act 2022*);

(v) the Inspector of the National Anti-Corruption Commission, or a person assisting the Inspector (within the meaning of the *National Anti-Corruption Commission Act 2022*); and

(b) the disclosure is for the purpose of that person exercising a power, or performing a function or duty.

(2) An entrusted person may make a record of or access protected information for the purpose of disclosing the protected information under subsection (1).

35 Disclosure etc. with consent

Consent of person to whom protected information relates

(1) An entrusted person may make a record of, disclose or access protected information that relates to the affairs of a person if:

(a) the person has expressly consented to the recording, disclosure or access; and

(b) the recording, disclosure or access is in accordance with that consent.

Consent of jurisdiction responsible for NDLFRS protected information

(2) An entrusted person may make a record of, disclose or access protected information that was:

(a) held in, or generated using, NDLFRS; and

(b) supplied by an authority of a State or Territory;

if the authority expressly consents to the recording, disclosure or access.

Note: The NDLFRS hosting agreement also contains privacy requirements that relate to the authority (see subsection 13(2)).

Part 5—Miscellaneous

36 Simplified outline of this Part

An object of this Act is to provide for oversight and scrutiny of the operation and management of the approved identity verification facilities. This Part provides for that oversight and scrutiny, as well as dealing with other miscellaneous matters.

The Secretary may delegate the Secretary's powers and functions under this Act.

The Secretary must publish certain documents relating to identity verification services, including the intergovernmental agreement, participation agreements, the NDLFRS hosting agreement and documents setting out access policies.

The Information Commissioner is to assess the approved identity verification facilities annually.

Annual reports must be prepared and tabled in Parliament about things done in connection with certain identity verification services.

An interim review and review of this Act must be conducted, both of which must be started within 2 years of the commencement of section 43 of this Act.

The Minister may make rules for the purposes of this Act, including rules for fees.

37 No requirement for individuals to identify themselves

(1) To avoid doubt, this Act does not affect whether individuals have the option of not identifying themselves, or of using pseudonyms, when dealing with another person or body.

Note: This Act does not affect the operation of Australian Privacy Principle 2 (about anonymity and pseudonymity).

(2) Subsection (1) does not affect the circumstances in which an identity verification service may be requested or provided.

38 Delegation of Secretary's powers and functions under this Act

(1) The Secretary may, in writing, delegate all or any of the Secretary's powers or functions under this Act to an SES employee or acting SES employee in the Department.

Note 1: ***SES employee*** and ***acting SES employee*** are defined in section 2B of the *Acts Interpretation Act 1901*.

Note 2: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain provisions relating to delegations.

(2) In performing a delegated function or exercising a delegated power, the delegate must comply with any written directions of the Secretary.

39 Publication of agreements and policies

(1) The Secretary must publish on the Department's website a copy of each of the following documents:

(a) the intergovernmental agreement;

(b) a participation agreement;

(c) the NDLFRS hosting agreement;

(d) an instrument that causes a person or body to become, or cease to be, a party to a participation agreement or the NDLFRS hosting agreement;

(e) a document that is approved by the Coordination Group provided for by the intergovernmental agreement and sets out an access policy for a service;

(f) a document varying, terminating or revoking a document described in paragraph (a), (b), (c), (d) or (e).

(2) However, the copy need not include part of the document if the Secretary considers that publication of the part:

(a) creates a risk to the security of identification information or an approved identity verification facility; or

(b) unreasonably discloses personal information that relates to an individual; or

(c) if the document is a participation agreement or a document described in paragraph (1)(e)—creates a risk to Australia's national security (within the meaning of the *National Security Information (Criminal and Civil Proceedings) Act 2004*).

(3) If the Secretary publishes the copy without part of the document because of subsection (2), the Secretary must publish on the Department's website written reasons for not publishing the part, except so far as publication of the reasons would create a risk described in subsection (2) or unreasonably disclose personal information.

40 Annual assessment by Information Commissioner

(1) The Information Commissioner has the function of doing both of the following within 6 months of the end of each financial year ending after the commencement of this section:

(a) assessing the approved identity verification facilities in relation to any act or practice of the Department during the financial year;

(b) giving the Secretary a written report on the assessment.

(2) For the purposes of the *Privacy Act 1988*, an assessment under subsection (1) of this section is taken to be an assessment under paragraph 33C(1)(a) of that Act.

41 Annual reporting

(1) The Secretary must give the Minister a report including the following information for each financial year ending after the commencement of this section:

(a) statistics relating to all requests in the financial year, by or on behalf of government authorities, for 1:1 matching services, broken down by:

(i) requesting authority (identified by name); and

(ii) the service requested; and

(iii) requests in response to which there was provided either information contained in, or associated with, a government identification document, or an indication of a match being the outcome of the comparison involved in the service; and

(iv) requests in response to which there was provided neither information contained in, or associated with, a government identification document nor an indication of a match being the outcome of the comparison involved in the service;

(b) statistics relating to all requests in the financial year from non-government entities for 1:1 matching services, including:

(i) the total number of those requests; and

(ii) the names of the non-government entities that made those requests; and

(iii) the number of those requests the response to which was that the requested comparison resulted in a match for an individual; and

(iv) the number of those requests the response to which was that the requested comparison did not result in a match for an individual;

(c) for 1:many matching services:

(i) the number of times that the service was used in the year; and

(ii) whether the requests were endorsed as required by section 17 or not;

(d) information about the accuracy of each system for biometric comparison of facial images that is operated by:

(i) the Department; or

(ii) the Department administered by the Minister administering the *Australian Passports Act 2005*;

for the purpose of providing identity verification services; or

(e) the following material relating to disclosures of identification information that were made in the financial year and were authorised by subsection 32(1) (about disclosures to lessen or prevent threats to life or health):

(i) the total number of disclosures;

(ii) the number of individuals whose identification information was disclosed;

(f) information about security incidents occurring in the financial year in connection with one or more of the approved identity verification facilities;

(g) information about actions taken in the financial year in response to security incidents that occurred (in the financial year or earlier) in connection with any of the approved identity verification facilities;

(h) information about data breaches connected with the operation of any of the approved identity verification facilities in the financial year;

(i) information about actions taken in the financial year in response to data breaches connected with the operation of any of the approved identity verification facilities in the financial year or earlier;

(j) information about termination or suspension in the financial year of the ability of a party to a participation agreement or the NDLFRS hosting agreement to request an identity verification service because the party does not or did not comply with the agreement or the access policy for the service;

(k) any other information that:

(i) relates to the financial year and either an identity verification service or the administration of this Act; and

(ii) is required by the Minister.

(2) The report must not unreasonably disclose personal information that relates to an individual.

Timing of annual report

(3) The Secretary must give the Minister the report as soon as practicable after the end of the financial year and in any case within 6 months after the end of the financial year.

Tabling of annual report

(4) The Minister must, subject to subsection (5), cause a copy of the report to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives the report.

(5) For the purposes of tabling the report, the Minister may make any deletions from the report as the Minister considers necessary to avoid prejudicing an investigation or compromising the operational activities of a Commonwealth, State or Territory government authority referred to in paragraph 17(1)(a).

42 Fees

(1) The rules may make provision relating to the imposition, collection and recovery of fees for either or both of the following:

(a) connections to the approved identity verification facilities, to allow the making of electronic communications to, and the receipt of electronic communications from, those facilities;

(b) requests for identity verification services.

(2) A fee must not be such as to amount to taxation.

43 Interim review, and review of this Act and provision of identity verification services

Interim review

(1A) The Minister must cause an interim review to be started as soon as practicable after 12 months, and before the end of 2 years, of the commencement of this section.

(1B) The interim review must consider the adequacy and operation of:

(a) the privacy protections contained in this Act; and

(b) the security requirements and obligations contained in this Act; and

(c) the penalties for non-compliance with obligations set out in participation agreements, including considering whether civil penalties should apply.

Review of Act and provision of identity verification services

(1) The Minister must cause a review of the operation of this Act and the provision of identity verification services to be started within 2 years of the commencement of this section.

Consultation, preparation and tabling of reports

(2A) The President of the Australian Human Rights Commission, the Human Rights Commissioner appointed under section 8B of the *Australian Human Rights Commission Act 1986*, and the Information Commissioner, must be consulted in relation to a review under subsection (1A) or (1).

(2) The Minister must cause a report of the review to be prepared and given to the Minister.

(3) The Minister must cause a copy of the report to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives the report.

44 Rules

(1) The Minister may, by legislative instrument, make rules prescribing matters:

(a) required or permitted by this Act to be prescribed by the rules; or

(b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(1A) Without limiting subsection (1), the rules may prescribe requirements relating to privacy with which a party to a participation agreement must comply.

Consultation on draft rules

(1B) Before making or amending any rules under subsection (1), the Minister must:

(a) cause to be published on the Department's website a notice:

(i) setting out the draft rules or amendments; and

(ii) inviting persons to make submissions to the Minister about the draft rules or amendments within the period specified in the notice (which must be at least 28 days after the notice is published); and

(b) if the rules deal with matters that relate to the privacy functions (within the meaning of the *Australian Information Commissioner Act 2010*)—consult the Information Commissioner; and

(c) consider any submissions received within the specified period.

(1C) The Minister may consider any submissions received after the specified period if the Minister considers it appropriate to do so.

Limitation on rules

(2) To avoid doubt, the rules may not do the following:

(a) create an offence or civil penalty;

(b) provide powers of:

(i) arrest or detention; or

(ii) entry, search or seizure;

(c) impose a tax;

(d) set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in this Act;

(e) directly amend the text of this Act.

Disallowance and sunsetting of rules

(3) Despite subsection 44(1) of the *Legislation Act 2003*, section 42 (disallowance) of that Act applies to the rules.

(4) Despite subsection 54(1) of the *Legislation Act 2003*, Part 4 of Chapter 3 (sunsetting) of that Act applies to the rules.

[*Minister's second reading speech made in—*
House of Representatives on 13 September 2023
Senate on 19 October 2023]

(117/23)