2022-2023

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

IDENTITY VERIFICATION SERVICES BILL 2023

IDENTITY VERIFICATION SERVICES (CONSEQUENTIAL AMENDMENTS) BILL 2023

EXPLANATORY MEMORANDUM

(Circulated by authority of the
Attorney-General, the Hon. Mark Dreyfus KC MP)

GLOSSARY

The following abbreviations and acronyms are used throughout this Explanatory Memorandum.

Abbreviation	***Definition***
Acts Interpretation Act	*Acts Interpretation Act 1901*
Australian Passports Act	*Australian Passports Act 2005*
Bill	Identity Verification Services Bill 2023
Citizenship Act	*Australian Citizenship Act 2007*
Consequential Amendments Bill	Identity Verification Services (Consequential Amendments) Bill 2023
Crimes Act	*Crimes Act 1914*
Crimes Regulations	Crimes Regulations 2019
Criminal Code	*Criminal Code Act 1995*
Department	the department responsible for administering the Act to be established by the Bill
DFAT	Department of Foreign Affairs and Trade
DVS	Document Verification Service
DVS hub	Document Verification Service hub
FIS	Face Identification Service
FMS hub	Face Matching Services hub
FVS	Face Verification Service
IGIS Act	*Inspector-General of Intelligence and Security Act 1986*
Intergovernmental agreement	*Intergovernmental Agreement on Identity Matching Services*
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
Legislation Act	*Legislation Act 2003*
Migration Act	*Migration Act 1958*
NDLFRS	National Drivers Licence Facial Recognition Solution
Ombudsman Act	*Ombudsman Act 1976*
Privacy Act	*Privacy Act 1988*
Secretary	Secretary of the department administering the Act to be established by the Bill
Witness Protection Act	*Witness Protection Act 1994*

GENERAL OUTLINE

1. Secure and efficient identity verification is critical to minimising the risk of identity fraud and theft, and protecting the privacy of Australians when seeking to access government and industry services and engage with the digital economy. The identity verification services are the only national capability that can be used by industry and government agencies to securely verify the identity of their customers.

2. Identity verification services are a series of automated national services offered by the Commonwealth to allow government agencies and industry to efficiently compare or verify personal information on identity documents against existing government records, such as passports, driver licences and birth certificates.

3. 1:1 matching services (the Document Verification Service and the Face Verification Service) are now used every day by Commonwealth, State and Territory government agencies and industry to securely verify the identity. In 2022, the DVS was used over 140 million times by approximately 2700 government and industry sector organisations, and there were approximately 2.6 million FVS transactions in the 2022-23 financial year.

4. Examples of the current uses of the DVS and FVS include:

- verifying the identity of an individual when establishing a myGovID to access online services, including services provided by the Australian Taxation Office
- financial service providers, such as banks, when seeking to verify the identity of their customers and to meet the 'know your customer' obligation under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
- Government agencies when providing services, disaster relief and welfare payments, and
- Commonwealth, state and territory government agencies verifying identity in order to provide or change credentials.

5. The Identity Verification Services Bill 2023 establishes new primary legislation that provides a legislative framework to support the operation of the identity verification services. The Bill will support the efficient and secure operation of the services without compromising the privacy of the Australian community.

6. The IVS Bill will:

- authorise 1:1 matching of identity through the identity verification services, with consent of the relevant individual, by public and private sector entities. This will be enabled by:
    - the Document Verification Service which provides 1:1 matching to verify biographic information (such as a name or date of birth), with consent, against government issued identification documents;
    - the Face Verification Service which provides 1:1 matching to verifiy biometric information (in this case a photograph or facial image of an individual), with consent, against a Commonwealth, state or territory issued identification document (for example, passports and driver licences); and
    - the National Driver Licence Facial Recognition Solution which enables the FVS to conduct 1:1 matching against State and Territory identification documents such as driver licences.
- authorise 1:many matching services through the Face Identification Service only for the purpose of protecting the identity of persons with a legally assumed identity, such as undercover officers and protected witnesses. The protection of legally assumed identities will also be supported by the use of the FVS. All other uses of 1:many matching through the identity verification services will not be authorised, and will therefore be prohibited.

- authorise the responsible Commonwealth department – in this case the Attorney-General's Department – to develop, operate and maintain the identity verification facilities (the DVS hub, the Face Matching Service Hub and the NDLFRS). These approved identity verification facilities will be used to provide the identity verification services. These facilities will relay electronic communications between persons and bodies for the purposes of requesting and providing identity verification services.

7. Subject to robust privacy safeguards, the Department will be authorised to collect, use and disclose identification information through the approved identity verification facilities for the purpose of providing identity verification services and developing, operating and maintaining the NDLFRS. Offences will apply to certain entrusted persons for the unauthorised recording, disclosing or accessing protected information.

8. The Bill ensures that the operation the identity verification services and requests for the use of those services are subject to privacy protections and safeguards. These include consent and notice requirements, privacy impact assessments, requirements to report security breaches and data breaches, complaints handling, annual compliance reporting and transparency about how information will be collected, used and disclosed. Furthermore, privacy law and/or the Australian Privacy Principles will apply to almost all entities that seek to make a request for identity verification services. These privacy protections and safeguards will be set out in participation agreements.

9. Government authorities that supply identification information that is used for the purpose of identity verification services will also be subject to the privacy protections and safeguards captured in the participation agreement. Breaches of participation agreements can lead to suspension or termination of the agreement, meaning that the entity would no longer be able to request identity verification services.

10. States or territories seeking to contribute to the NDLFRS will be subject to privacy obligations and safeguards, which are required by the Bill and will be set out in the NDLFRS hosting agreement.

11. The Bill requires parties to the agreement to agree to be bound by the Privacy Act or a state or territory equivalent, or agree to be subject to the Australian Privacy Principles. The Bill requires state or territory authorities to inform individuals if their information is stored on the NDLFRS (and provide for a mechanism by which those persons can correct any errors), inform the Department and individuals whose information is stored on the NDLFRS of any data breaches, establish a complaints mechanism, and report annually to the Department on the party's compliance with the agreement. The Bill enables states and territories to limit the use of identity information stored on the NDLFRS, and requires the Department to maintain the security of the NDLFRS. The Department may suspend or terminate access to the NDLFRS in the event of a party's non-compliance with legislative obligations.

12. To protect the privacy of Australians, the Department will be required to maintain the security of electronic communications to and from the approved identity verification facilities, and the information held in the NDLFRS. This information and communications must be encrypted and data breaches reported.

13. There will be transparency about the operation of the approved identity verification facilities, including through extensive annual reporting requirements and annual assessments by the Information Commissioner on the operation and management of the facilities.

14. The Bill reflects and seeks to implement aspects of the Commonwealth's commitments under the *Intergovernmental Agreement on Identity Matching Services* (Intergovernmental Agreement). The Intergovernmental Agreement provides that jurisdictions would share and match biographic and biometric information, with robust privacy safeguards, through the identity verification services.

12. The Bill will be supported by the Identity Verification Services (Consequential Amendments) Bill which amends the *Australian Passports Act 2005* to provide a clear legal basis for the Minister to

disclose personal information for the purpose of participating in one of the following services to share or match information relating to the identity of a person:

- the DVS or the FVS, or
- any other service, specified or of a kind specified in the Minister's determination.

13. The Consequential Amendments Bill will also allow for automated disclosures of personal information to a specified person via the DVS or the FVS. In combination, this comprehensively authorises the operation of the DVS and FVS in relation to Australian travel documents regulated by the Australian Passports Act.

FINANCIAL IMPACT STATEMENT

14. The financial impact of the Bill is low. The Bill provides for the charging of fees for requests for identity verification services.

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Identity Verification Services Bill 2023

15. This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Bill

16. Secure and efficient identity verification is critical to preventing identity fraud and theft, and protecting industry, governments and the wider Australian community when engaging with the digital economy.

17. The identity verification services are the only national capability that can be used by industry and government agencies to securely verify the identity of their customers. These services enable Australians to engage with the digital economy and access critical services without exposing them to identity fraud and theft.

18. The Identity Verification Services Bill 2023 provides a legislative framework to support the continued operation of these services and ensures they are subject to robust safeguards and security measures. This framework will:

- authorise 1:1 matching of identity through the identity verification services, with consent of the relevant individual, for transactions with public and private sector entities. This will be enabled by:
    - the Document Verification Service (DVS) which provides 1:1 matching to verify biographic information (such as a name or date of birth), with consent, against government issued identity credentials;
    - the Face Verification Service (FVS) which provides 1:1 matching to verifiy of biometric information (in this case a photograph of an individual), with consent, against a Commonwealth, state or territory issued identity credential (for example, passports and driver licences); and
    - the National Driver Licence Facial Recognition Solution (NDLFRS) which enables the FVS to conduct matching against State and Territory credentials such as driver licences.
- limit the use of 1:many matching services to the Face Identification Service (FIS) which can only be used when required to protect the identity of persons with a legally assumed identity, such as undercover officers and witnesses in protection programs. The protection of legally assumed identities will also be support by the use of the FVS. All other 1:many matching through the identity verification services will not be authorised, and is therefore prohibited.

  This capability will provide an efficient and secure way to check that the true identity of a person with a legally assumed identity is not exposed, either unintentionally or by nefarious actors. Such exposure would compromise the safety and security of individuals and their families, and undermine law enforcement and intelligence operations.
- authorise the responsible Commonwealth department – in this case the Attorney-General's Department – to operate and maintain the identity verification services. This includes operating the DVS hub, the Face Matching Services Hub and the NDLFRS which will enable the secure relaying of electronic communications made in the course of requesting and providing the identity verification services.

Human rights implications

19. The Bill engages the following rights contained in the International Covenant on Civil and Political Rights:

- the right to equality and non-discrimination contained in Article 2
- the protection against arbitrary or unlawful interference with privacy contained in Article 17, and
- The right to freedom of expression contained in Article 19.

20. The Bill engages the right to social security contained in Article 9 of the International Covenant on Economic, Social and Cultural Rights.

The right to equality and non-discrimination contained in Article 2 of the ICCPR

21. Article 2 of the ICCPR requires states to ensure that individuals are not subject to discrimination on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Where not provided states must undertake necessary steps to ensure equality.

22. The Bill promotes this right by providing for the NDLFRS which will allow for a broader range of persons to have their identity verified through the identity verification services. The NDLFRS supports the continued operation of the FVS as it provides the technical capability for biometric matching to occur against State and Territory credentials.

23. It will allow more Australians to securely access critical services online noting that approximately 80 per cent of Australians have a driver licence. For example, the Bill ensures Australians can have their identity verified against their driver licence in order to establish a 'strong' MyGovID which is needed to access certain government services, such as those provided by Centrelink and the Australian Tax Office. Without the NDLFRS, only persons with an Australian Passport, which accounts for approximately 50 per cent of the population, would be able to create a 'strong' MyGovID and access critical services.

24. Furthermore, subclause 6(4) of the Bill ensures certain types of information are excluded and cannot be sought or requested through the identity verification services. This information is:

- information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a trade union, sexual orientation or practices, or criminal record (paragraph (a))
- health information about an individual (as defined in section 6FA of the Privacy Act) (paragraph (b)), and
- genetic information about an individual (paragraph (c))

Protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR

25. Article 17 of the ICCPR prohibits arbitrary or unlawful interference with a person's privacy, family, home or correspondence and unlawful attacks on a person's honour or reputation. It also provides that everyone has the right to the protection of the law against such interference or attacks.

26. The right to privacy articulated in Article 17 may be subject to permissible limitations that are authorised by law, are not arbitrary, pursue a legitimate objective, are necessary to achieve that objective, and are a proportionate means of achieving it. In order for an interference with the right to privacy not to be arbitrary, the interference must be for a reason consistent with the provisions, aims and objectives of the ICCPR and be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted 'reasonableness' in this context to mean that 'any

interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case'.[1]

27. The Bill engages Article 17 by authorising the Department to collect, use and disclose personal or sensitive information captured under the definition of identification information for the purposes of providing the identity verification services. The privacy, accountability and transparency measures contained in the Bill provide appropriate safeguards against any limitations on the right to privacy as a result of the identity verification services provided for by the Bill. This ensures that privacy is an ongoing and primary consideration in the implementation of the Bill and the identity verification services.

28. Additional restrictions on the availability and uses of the identity verification services, and the benefits they provide to the Australian community further ensures that the limitations on the right to privacy resulting from each service are reasonable, necessary and proportionate to the legitimate objectives of the particular service.

Verifying identity through the DVS and FVS

29. The Bill enables government and non-government organisations that are parties to a participation agreement to make a request for the DVS and FVS for the purposes of verifying the identity of a person. When servicing such a request, the Department will use and disclose identification information (which includes personal and sensitive information within the meanings of the *Privacy Act 1988*).

30. The DVS and FVS are critical services that enable the Australian community to securely access government and industry services without exposing individuals to identity fraud and theft. Without the DVS and FVS, the privacy of Australians may be compromised when seeking to access online services as there is no alternative national system to securely verify identity.

31. Accordingly, any limitation on the right to privacy is proportionate to the benefit these services provide in supporting Australians to access the digital economy and critical industry and government services.

32. Currently, the DVS and FVS are used in the following circumstances:

- verifying the identity of an individual when establishing a myGovID to access online services, including services provided by the Australian Taxation Office
- financial service providers, such as banks, when seeking to verify the identity of their customers and to meet the 'know your customer' obligation under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
- Government agencies when providing services, disaster relief and welfare payments, and
- Commonwealth, state and territory government agencies verifying identity in order to provide or change credentials.

33. Furthermore, a number of privacy safeguards are included in the Bill to ensure the operation of the DVS and FVS is reasonable and limited to certain functions. These privacy safeguards include:

- a DVS request will only relate to *DVS information* (see subclause 6(3)) which is information on a government identification document except for a photograph
- a private sector organisation is limited to receiving either a 'match' or 'no match' response in relation to an FVS request (see subclause 19(d)). This means that the requesting agency will not receive additional information about the individual

[1] United Nations Human Rights Committee, *The right to privacy in the digital age*, UN Doc A/HRC/27/37, 30 June 2014, paragraph 21, quoting United Nations Human Rights Committee, *Toonan v. Australia*, Communication No. 488/1992, paragraph 8.3.

- when seeking to verify identity, the requesting agency must obtain the consent of the individual (see subclause 9(2)(b)), and
- requesting agencies must be a party to a participation agreement (see subclause 15(1)(b) and subclause 19(a)). The privacy protections in the participation agreement are discussed below.

34. When obtain consent, entities are also required to notify individuals of certain matters (see subclause 9(3)). This supports the individual's right to privacy as it ensures consent is fully informed and provided after considering certain key matters, including:

- how the party seeking consent uses identity verification services and how any facial images collected by that party for the purpose of making a request for services will be used and disposed of (subclause 9(3)(a) and (b)).
- what legal obligations the party seeking to collect identification information has in relation to that collection, what rights an individual has and what the consequences of declining to give consent are (subclause 9(3)(d), (e) and (f))

Face Identification Service (FIS)

35. The FIS is a 1:many matching service. The Bill will only authorise the use of the FIS by officers from a limited group of Commonwealth, State and Territory agencies for the purpose of protecting the identity of shielded persons and their associates. Shielded persons are defined in clause 5 and, generally speaking, include those persons who have been authorised to acquire or use an assumed identity (for example, an undercover police officer) under law, including the *Crimes Act 1914* (Cth) and *Witness Protection Act 1994* (Cth). The Bill does not authorise the FIS to be used for any other purposes, which limits any impact on the right to privacy.

36. The limitations on the right to privacy involved in 1:many matching through the FIS are reasonable and proportionate given the importance of the FIS in protecting the identity or identities of shielded persons or associates of shielded persons.

37. For example, a FIS request may be submitted in regards to an officer from a law enforcement agency who will be going undercover to infiltrate a criminal organisation and, accordingly, has been authorised to acquire an assumed identity under Part IAC of the Crimes Act. In this instance, the FIS request will allow for the officer's digital photo to be searched across data holding agencies to determine if the undercover officer has a government identification document (like a driver licence) under their true identity or a different identity which may have been used in a previous undercover operation. If a match has been identified, the law enforcement agency will be able to work with relevant agencies to ensure the government identification document for the undercover officer is not accessible for identity verification purposes via a DVS or FVS search.

38. The FIS will support relevant agencies to identity whether the identity of an undercover officer could be compromised by a criminal organisation. This could compromise an active investigation and undermine the safety of an undercover officer and their family.

39. A request to use the FIS is subjected to a number of safeguards and limitations, which ensures its use is reasonable and proportionate. These safeguards and limitations include:

- the request for a FIS must be made by an officer on behalf of one of the Commonwealth, State or Territory government authorities listed in paragraph 17(1)(a) for the purpose of protecting the identity of a shielded person or someone else associated with a shielded person (subclause 17(1))
- the person making the request for a FIS 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) (subclause 17(2))
- the request must have specific characteristics and include a single facial image of an individual (subclause 17(3))

- the request for a FIS must be endorsed by a senior officer of the same government authority (subclause 17(4))
- a person must not endorse a request made on behalf of an authority unless satisfied that the request is made for the purposes of protecting a shielded person, or associate, stated in the request, and the performance of the authority's functions (subclause 17(5)), and
- require parties to the participation agreement who are government agencies to not permit an individual who is an officer, staff member, employee or contractor of that agency to receive any facial images by way of a response to an identity verification service or deal with a facial image provided in response to such a request unless the individual has been trained in facial recognition and image comparison (subclause 10(2)(b)).

Privacy protections in the participation agreement

40. The Bill contains robust privacy protections and safeguards, which will be captured in a participation agreement. The agreement outlines the respective roles, rights and obligations to each party when participating in, and accessing and using, the identity verification services. The Bill requires participation agreements to include minimum security standards, privacy obligations and reporting requirements for each party.

41. Non-compliance with a participation agreement may cause parties to the agreement to have their use and access to the identity verification services suspended or terminated

42. This is a significant penalty and will support compliance and act as deterrent to non-compliance given the importance of the identity verification services to government and industry.

43. All entities accessing identity verification services will be required to be a party to a participation agreement in respect of the relevant service. Parties to the agreement will include:

- the Department as the administrator and operator of the identity verification services on behalf of the Commonwealth, and
- non-government organisations and Commonwealth, State and Territory government agencies that wish to make requests or make information available for relevant services offered under the identity verification services.

44. In order to be a party to a participation agreement, an entity must (see subclause 9(1)):

- be subject to the Privacy Act
- be subject to a privacy law of a State or Territory, where that law is prescribed by the in the rules
- have agreed to comply with the Australian Privacy Principles, with any modifications of Australian Privacy Principles 7.8 and 12.2 (about laws of the Commonwealth) specified in the agreement, as if the entity were an 'APP entity' within the meaning in section 6 of the Privacy Act
- the entity is a government authority prescribed by the Minister in rules, or
- 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* (NZ).

45. The Bill includes a number of important safeguards and protections to ensure privacy considerations are taken into regard when using the identity verification services. For example, through the participation agreements, the Bill requires requesting agencies to:

- provide for privacy impact assessments (as defined in subsection 33D(3) of the Privacy Act) of requesting identity verification services (subclause 9(2)(a))

- provide for the obtaining of an individual's 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 the request is made for the purpose of protecting a shielded person) (subclause 9(2)(b))
- providing information to a person from whom such consent is sought about:
    - how the party seeking consent uses identity verification information
    - how any facial images will be used and disposed of
    - whether facial images will be retained or used for any other purposes
    - what legal obligations the party seeking to collect the identification information has in relation to that collection
    - what rights the individual has in relation to the collection of the identification information
    - the consequences of the individual declining to consent
    - where the individual can get information about making complaints, and
    - where the individual can get information about the operation and management of the approved identification verification facilities. (subclause 9(c) and (9(3))
- establish and maintain arrangements for dealing with complaints by individuals whose identification information is held by the party (paragraph 9(2)(d));
- notify the Department of any breaches of security in relation to the identity verification services (paragraph 9(2)(d))

46. The Department will be required to inform the Information Commissioner of a breach of security that is reported to the Department (as a result of subclause 9(2)(e)) and is a data breach that is reasonably likely to result in serious harm to an individual whose identification information is involved in the breach. This obligation is intended to align with, and be read in a manner consistent with, the notifiable data breach scheme under the Privacy Act.

47. Participation agreements also prevent disclosures of identification information obtained as a result of an identity verification service, subject to limited and reasonable exceptions including where required by law or permitted by law, or in accordance with the participation agreement (subclause 10(2)(a)(i) and (ii)).

48. Participation agreements that provide for government authorities to make available identification information for an identity verification service will also be able to limit the use of that information (clause 11).

49. Participation agreements will also have extensive compliance requirements and must be subject to annual auditing of compliance with the agreement. The outcome of these audits will need to be reported to the Department (subclause 12(a) and (b)).

Privacy protections in the NDLFRS hosting agreement

50. The Bill includes a number of privacy obligations and safeguards in order to protect identification information on databases on the NDLFRS. These obligations and safeguards are reflected in the NDLFRS hosting agreement which is a written agreement between the Department (representing the Commonwealth) and each authority of a State or Territory that supplies or proposes to supply identification information to the Department for inclusion in a database in the NDLFRS (see clause 13).

51. Subclause 13(2) requires all parties to the agreement to either be subject to a privacy law, or agrees to be bound by privacy obligations. Importantly, this means that the parties have obligations

with respect to collection, use and disclosure of personal information, and in relation to access to and correct of such information, that apply to each party to the agreement.

52. The NDLFRS hosting agreement also requires participating States and Territories to satisfy certain privacy obligations, including:

- taking reasonable steps to inform each individual whose identification information is, or is to be, included in a database in the NDLFRS of that inclusion (subclause 13(3)(a));
- provide each individual whose identification information is included in a database in the NDLFRS with a means of finding out what that information is and having any errors in that information corrected (subclause 13(3)(b));
- inform each such individual and the Department of any data breaches that involve identification information about the individual and the NDLFRS and are reasonably likely to result in serious harm to the individual (subclause 13(3)(c)); and
- provide means for dealing with complaints by individuals relating to the NDLFRS and identification information about them that is included in a database in the NDLFRS (subclause 13(3)(d)).

53. The NDLFRS hosting agreement also requires the Department to:

- maintain the security of identification information included in a database in the NDLFRS, including by encrypting the information (subclause 13(4)(a))
- inform the other parties to the agreement of any data breaches involving that information and the NDLFRS (subclause 13(4)(b)), and
- inform the Information Commissioner of any data breaches that involve information and the NDLFRS, and are reasonably likely to result in serious harm to an individual to whom that information relates (paragraph 13(4)(c)).

54. These safeguards and protections ensure that any limitations on the right to privacy as a result of the NDLFRS are reasonable and proportionate, particularly given the benefits the NDLFRS provides to the Australian community.

The scope of the Department's authority to operate the identity verification services

55. Clause 25 authorises the Department to develop, operate and maintain the approved identity verification facilities. In developing, operating and maintaining the facilities, the Bill places a number of important obligations on the Department in order to protect the privacy of individuals. The Department must:

- maintain the security of identification information included in a database in the NDLFRS, including by encrypting the information (subclause 13(4)(a)
- maintain the security of electronic communications to and from the approved identity verification facilities, including by encrypting the information (subclause 25(a)), and
- protect the information from unauthorised interference or unauthorised access (subclause 25(b)).

56. These are important safeguards, and require the Department to maintain the security of the identification information included in databases in the NDLFRS and information flows to and from the approved identity verification facilities, including by using encryption. These requirements will ensure the Department implements appropriate security measures to protect personal and sensitive information, and prevent unauthorised interference or access.

57. The Bill also contains a number of additional transparency, accountability and oversight measures to ensure privacy standards are upheld. These include:

- the requirement to a publish participation agreement, the NDLFRS hosting agreement and other relevant documents on the Department's website (clause 39)
- providing for entrusted persons to disclose protected information to an Inspector-General of Intelligence and Security (IGIS) official or a Commonwealth Ombudsman official, to assist either agency to exercise its functions to oversee the use of identity verification services by agencies using the services (clauses 33 and 34)
- annual assessments by the Information Commissioner of the operation and management of the identity verification services by the Department (clause 40)
- annual reporting requirements, including providing information in the report about data breaches and security incidents, and the accuracy of facial recognition systems. The annual report will be provided to the Minister and tabled in each House of Parliament (clause 41), and
- the requirement to commence a review of the operation of the Bill and the provision of identity verification services within 2 years of the commencement of the Bill (clause 43).

The right to freedom of expression contained in Article 19 of the ICCPR

58. Article 19 of the ICCPR provides that everyone shall have the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds.

59. Article 19(3) of the ICCPR provides that this right may be limited on grounds including respect for the rights of others, or the protection of national security or public order. Any limitations must be prescribed by legislation and be reasonable, necessary, and proportionate to achieve the desired purpose.

60. The Bill engages the right to freedom of expression by making it an offence for an entrusted person (as defined in clause 30(4)) to make a record of, disclose, or access protected information (see clause 30). An ***entrusted person*** means:

- the Secretary of the Department
- APS employees (as defined in section 7 of the *Public Service Act 1999*) in the Department
- a person whose services are made available to the Department who is:
  - an employee of an Agency as defined in the *Public Service Act 1999*
  - or an officer or employee of a State or Territory
  - an officer or employee of a government authority (defined in clause 5 to mean an authority of the Commonwealth, state or territory but not a local government authority)
  - an officer or employee of the government of a foreign country or an authority of a foreign country,
  - or an officer or employee of a public international organisation as defined in section 70.1 of the Criminal Code (for example multilateral international organisations such as the World Bank, World Trade Organization and International Monetary Fund)
- a contractor engaged to provide services to the Department in connection with an approved identity verification facility (whether the contractor is engaged directly or as a subcontractor), or

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

61. ***Protected information*** means any of the following:

- information obtained by an entrusted person from electronic communications to or from an approved identity verification facility, or from the NDLFRS
- information about the making, content or addressing of an electronic communication to or from an identity verification facility that was obtained by an entrusted person in their capacity as an entrusted person
- information about identification information relating to a particular individual held in, or generated using, the NDLFRS, that was obtained by an entrusted person in their capacity as an entrusted person, and
- information obtained by an entrusted person in their capacity as an entrusted person that would enable access to the DVS hub, Face Matching Services hub or the NDLFRS.

62. The offences only limit the right to freedom of expression to the extent necessary to protect the information from unauthorised disclosure, including by distinguishing between entrusted persons who are subject to the offence provision, and other persons who are not. The definition of entrusted persons is limited to officers who are working, in some capacity, in the Department. It will not apply to any other persons. This is an appropriate limitation, given such persons will have chosen to take on such roles and received training and induction about the sensitivity of the information and services that they are dealing with, and the application of the offences.

63. The offences also only apply to protected information as defined in subclause 30(4). This is limited to information held or generated using an approved identity verification facility, or that would enable access to such facilities. This information is sensitive and needs to be protected in order to ensure the security of the facilities and support the privacy safeguards set out in the Bill.

64. An entrusted person will not be able to inadvertently commit the offences, given that the fault element of intention will apply to the conduct elements and the fault element of recklessness will apply to the other fault elements.

65. Clause 30 creates specific exceptions to the offences set out in subclauses 30(1) and (2).

66. These exceptions apply in addition to the general defences available under Part 2.3 of the Criminal Code and the authorisations set out in clauses 31, 32, 33, 34 and 35 of the Bill. These exceptions ensure that an entrusted person will not be inappropriately subject to criminal liability for their conduct where:

- their conduct was authorised by a law of the Commonwealth or of a state or territory
- their conduct was in compliance with a requirement under a law of the Commonwealth or of a state or territory
- they were performing their functions or duties or exercising a power related to an approved identity verification facility
- they reasonably believed that it is necessary to prevent a serious or imminent threat to the health or life of a person and the disclosure was made for the purpose of preventing or lessening that threat
- they were disclosing protected information to an IGIS official for the purpose of the IGIS official exercising a power, or performing a duty, as an IGIS official
- they were disclosing protected information to an Ombudsman official for the purpose of the Ombudsman official exercising a power, or performing a function or duty, as an Ombudsman official

- they had obtained the consent of the person to whom the protect information relates, or
- the protected information that was held in, or generated using the NDLFRS, was supplied by an authority of a State or Territory and that authority has consented to the recording, disclosure or access.

67. This limitation is reasonable given the sensitive nature of the information to which entrusted persons will have access, and implications for an individual if their identification information is unnecessarily disclosed. The limitation is proportionate to protect the privacy of individuals, and is one of the key privacy safeguards built into the Bill.

The right to social security contained in Article 9 of ICESCR

68. Article 9 of the ICESCR establishes the right to social security and insurance.

69. The provision of welfare payments and other benefits are contingent on identity verification in order to ensure welfare is provided to the correct people and to prevent fraud and misuse of government funds. By making identity verification more accessible, this Bill will reduce the administrative burden on those seeking services, support the fast, secure and private provision of such services, and have a positive impact on the right to social security.

Conclusion

70. The Bill is compatible with human rights. To the extent that it may limit human rights, particularly the right to privacy, those limitations are reasonable, necessary and proportionate to achieving that objective.

Identity Verification Services (Consequential Amendments) Bill

71. The Consequential Amendments Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Bill

72. The Consequential Amendments Bill amends the *Australian Passports Act 2005* to provide a clear legal basis for the Minister to disclose personal information for the purpose of participating in one of the following services to share or match information relating to the identity of a person:

- the Document Verification Service or the Face Verification Service (new paragraphs 46(1)(da)(i) to (ii)), or
- any other service, specified or of a kind specified in the Minister's determination (new paragraph 46(da)(iii)).

73. The Consequential Amendments Bill will also allow for automated disclosures of personal information to a specified person via the Document Verification Service or the Face Verification Service.

74. In combination, this comprehensively authorises the operation of the Document Verification Service and Face Verification Service in relation to Australian travel documents regulated by the Australian Passports Act.

Human rights implications

75. The Consequential Amendments Bill engages the protection against arbitrary or unlawful interference with privacy contained in Article 17 in the International Covenant on Civil and Political Rights and the right to social security contained in Article 9 of the International Covenant on Economic, Social and Cultural Rights.

Protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR

76. Article 17 of the ICCPR prohibits arbitrary or unlawful interference with a person's privacy, family, home or correspondence and unlawful attacks on a person's honour or reputation. It also provides that everyone has the right to the protection of the law against such interference or attacks.

77. The right to privacy articulated in Article 17 may be subject to permissible limitations that are authorised by law, are not arbitrary, pursue a legitimate objective, are necessary to achieve that objective, and are a proportionate means of achieving it. In order for an interference with the right to privacy not to be arbitrary, the interference must be for a reason consistent with the provisions, aims and objectives of the ICCPR and be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted 'reasonableness' in this context to mean that 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case'.2

78. The Consequential Amendments Bill engages Article 17 by inserting:

- new paragraph 46(1)(da) into the Australian Passports Act to allow the Minister to disclose personal information for the purposes of the Document Verification Service (DVS) and Face Verification Service (FVS), and
- new section 46A to clarify and enable automated disclosure of information for the purposes of new paragraph 46(1)(da), including the DVS and FVS.

79. The Consequential Amendments Bill, the Australian Passports Act and the Privacy Act provide safeguards and limitations to protect privacy in relation to the proposes amendments. Furthermore, the overall benefits to the Australian community from these amendments ensures that any limitation on the right to privacy resulting from these amendments is reasonable, necessary and proportionate.

Limitations on the application of the amendments

80. New paragraph 46(1)(da) and new section 46A, in combination, authorise the Minister to disclose personal information to specified persons, using automated systems, for the purposes of the DVS and FVS. This aligns with the current operational needs of the Department of Foreign Affairs and Trade and ensures that, in all other circumstance, the appropriateness, necessity and legal authority to support disclosures of personal information is considered by a decision-maker in DFAT or the Minister.

81. These amendments do not allow for the automated disclosure of personal information to the Face Identification Service (FIS). This an important limitation that reduces any impact on the right to privacy. The FIS is a relatively more privacy intrusive identity verification service noting that the DVS and FVS are 1:1 matching services that are mostly used to verify an individual's identity with consent. While the operation of the FIS is limited and subject to safeguards and protections in the Bill, the FIS is a 1:many matching identity verification service that is used to match a facial image of a person against images of persons held across government records.

Privacy protections and safeguards

82. As reflected in the note at the end of the current section 46 of the Australian Passports Act, information disclosed under new paragraph 46(1)(da) must be dealt with in accordance with the Australian Privacy Principles. This means that, for example, Australian Privacy Principle 6 would apply, which will place limitations on the use or disclosure of personal information that was collected as a result of new paragraph 46(1)(da).

---

[2] UNHRC, *The right to privacy in the digital age*, UN Doc A/HRC/27/37, 30 June 2014, paragraph 21, quoting United Nations Human Rights Committee, *Toonen v. Australia*, Communication No. 488/1992, paragraph 8.3.

83. The Bill also includes a range of safeguards and limitations to ensure that the disclosure of personal information as a result of new paragraph 46(1)(da) for the purposes of the DVS and FVS is reasonable and proportionate.

84. These privacy safeguards and limitations include:

- a DVS request will only relate to DVS information (see subclause 6(3) of the Bill) which is information on a government identification document except for a photograph
- a private sector organisation is limited to receiving either a 'match' or 'no match' response in relation to an FVS request (see subclause 19(d) of the Bill). This means that the requesting agency will not receive additional information about the individual
- when seeking to verify identity, the requesting agency must obtain the consent of the individual (see subclause 9(2)(b) of the Bill), and
- requesting agencies must be a party to a participation agreement (see subclause 15(1)(b) and subclause 19(a) of the Bill). The participation agreement also includes a number of additional privacy.

85. The Bill includes a number of important safeguards and protections to ensure privacy considerations are taken into regard when using the identity verification services. For example, the participation agreements requires requesting agencies to:

- provide for privacy impact assessments (as defined in subsection 33D(3) of the Privacy Act) of requesting identity verification services (subclause 9(2)(a))
- establish and maintain arrangements for dealing with complaints by individuals whose identification information is held by the party (paragraph 9(2)(d));
- notify the Department of any breaches of security in relation to the identity verification services (paragraph 9(2)(d)).

86. These and other privacy, accountability and transparency measures in the Bill provide appropriate safeguards against unnecessary impositions on the right to privacy as a result of the Minister making Australian travel document data available for all the purposes of the identity verification services.

Benefits to the Australian community

87. Any limitations on the right to privacy from the proposed amendments to the Australian Passports Act are reasonable and proportionate given the benefits they will provide to the Australian community.

88. New paragraph 46(1)(da) and new section 46A will enable government agencies and industry organisations to verify their customer's identity through an Australian Passport, which is the only government issued identity credential that enables biometric verification

89. Biometric verification is a highly secure way of verifying identity and is currently required to create a 'strong' MyGovID which is needed to access certain Centrelink and Australian Tax Office services.

90. Automated disclosures of personal information will also support the continued operation of the identity verification services which is critical to support access to industry and government services without exposing individuals to identity theft and fraud.

The right to social security contained in Article 9 of ICESCR

91. Article 9 of the ICESCR establishes the right to social security and insurance.

92. The provision of welfare payments and other benefits are contingent on identity verification in order to ensure welfare is provided to the correct people and to prevent fraud and misuse of government funds.

93. The Consequential Amendments Bill will promote the right to social security by enabling the biometric verification of identity which is currently needed to access certain Centrelink services.

Conclusion

94. The Bill is compatible with human rights. To the extent that it may limit human rights, particularly the right to privacy, those limitations are reasonable, necessary and proportionate to achieving that objective

IDENTITY VERIFICATION SERVICES BILL 2023

NOTES ON CLAUSES

Part 1—Preliminary

Division 1—Preliminary

Clause 1—Short Title

95. This clause provides for the short title of the Act to be enacted by the Bill to be the *Identity Verification Services Act 2023*.

Clause 2—Commencement

96. This clause provides for the commencement of each provision in the Bill as set out in the table. Item 1 in the table provides that the whole of the Bill will commence on the day after the Bill receives Royal Assent.

Clause 3—Objects of this Act

97. This clause outlines the objects of the Bill. As section 15AA of the Acts Interpretation Act provides that statutes should be interpreted in accordance with their objects, all the other provisions of the Bill are to be read, as far as is possible, as being designed to carry out these objects. This clause provides that the objects of the Bill are to:

- authorise the Secretary to develop, operate and maintain the three approved identity verification facilities, namely the DVS hub, the FMS hub and the NDLFRS (paragraph (a));
- authorise the Department, but not other persons or bodies, to collect, use and disclose identification information that has been communicated to an approved identity verification service, or generated using the NDLRFS, relating to certain purposes: the use of 1:1 verification services for verifying the identity of an individual; or the use of 1:many verification services for protecting shielded persons or someone else associated with a shielded person (paragraph (b));
- protect information that has been communicated to identity verification facilities and other information relating to the use and security of those facilities, from unauthorised recording or disclosure by people who work for the Department (paragraph (c)); and
- provide for oversight and scrutiny of the operation and management of the approved identity verification facilities by the Department (paragraph (d)).

Authorising the operation of the identity verification facilities

98. The Bill provides the Department with legislative authority for the operation of the three identity verification facilities—the DVS hub, the FMS hub and the NDLFRS. These facilities are technical components that enable the operation of the identity verification services. They support the secure communication of requests and the outcome of those requests between those organisations making a request and data holding agencies.

99. In developing, operating and maintaining the facilities, the Department will be required to maintain the security of electronic communications to and from the facilities, including by encrypting the information and protecting the information from unauthorized interference or access.

Authorising the Department to collect, use and disclose identification information

100. The Bill authorises the Department to collect identification information (as defined in clause 5) for the purposes of:

- providing a DVS or FVS for the purpose of verifying the identity of a person

- providing a FVS or FIS for the purpose of protecting a shielded person or someone else associated with a shielded person
- developing identity verification services or facilities for providing these services, and
- developing, operating or maintaining the NDLFRS.

101. This ensures that the collection of identification information is authorised for the purposes of the Australian Privacy Principles.

102. The Bill also authorises the Department to, for the purposes set out above, use and disclose identification information that has been collected by means of an electronic communication to an approved identification verification facility or is held in, or generated using, the NDLFRS. This ensures that such use and disclosure is authorised for the purposes of the Australian Privacy Principles.

Protecting identification information communicated to identity verification facilities

103. The Bill ensures that information connected with an identity verification facility is appropriately protected from unauthorised access by entrusted persons. The Bill contains criminal offences applying to entrusted persons within the Department. These offences relate to protected information, which includes identification information obtained from identity verification facilities or the NDLFRS, information about the making of communications to the facilities or the NDLFRS or information enabling access to the facilities. The offences apply where an entrusted person accesses, makes a record of, or discloses, such information.

Oversight and scrutiny of the operation and management of identity verification facilities

104. The Bill provides for appropriate oversight and scrutiny of the operation and management of identity verification facilities. This includes requirements to publish relevant agreements and policies, an annual assessment by the Information Commissioner and extensive annual reporting.

Clause 4—Simplified outline of this Act

105. This clause provides a simplified outline of the Bill, including the operation of the identity verification facilities and the services that are authorised to be conducted using those facilities.

106. The simplified outline is included to assist readers to understand the substantive provisions of the Bill. The outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of the Bill.

Division 2—Definitions

Subdivision A—General definitions

Clause 5—Definitions

107. This clause sets out the Dictionary for the Bill and defines the following terms.

108. ***1:1 matching service*** means the DVS or the FVS, which are separately defined in clauses 15 and 19, respectively. The definition of 1:1 matching service is relevant to the definition of ***identity verification service*** in this clause. 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. Under the Bill, 1:1 matching services can be used for verifying the identity of an individual or, in the case of the FVS, for protecting shielded persons.

109. ***1:many matching service*** means the FIS, which is separately defined in clause 16. The definition of 1:1 matching service is relevant to the definition of ***identity verification service*** in this clause. A 1:many matching service compares a facial image (such as a photograph) against other facial images. Under the Bill, 1:many matching services can only be used for protecting shielded persons.

110. ***Access policy*** is defined in clause 14 of the Bill. Parties to participation agreements must comply with relevant access policies in order to have access to identity verification services. The Bill

will require access policies to be published (subclause 39(1)(e)) and information about compliance with access policies must be included in the annual report (subclause 41(1)(k)).

111. ***Approved identity verification facility*** means the DVS hub, the Face Matching Service Hub and the NDLFRS, which are separately defined in this clause. This definition is required because, under Part 2 of the Bill, the Secretary will be authorised to develop, operate and maintain the approved identity verification facilities. Further, under Part 3 of the Bill, the Department is authorised to use and disclose information obtained from an electronic communication to or from an approved identity verification facility.

112. ***Data breach*** means an occurrence of unauthorised access to, unauthorised disclosure of or loss of identification information. This definition is required because the participation agreements and NDLFRS Hosting Agreement must contain reporting obligations in the event of a data breach. The Department must inform the Information Commissioner of any breach of security that is reasonably likely to result in serious harm to the individual whose identification information is involved in the breach. The annual report must also include information on the occurrence of any data breaches connected with the operation of an approved identity verification facility in the financial year and any actions taken in response.

113. ***DVS*** is defined in clause 15 of the Bill. The DVS, also known as the Document Verification Service, is a 1:1 matching service that performs biographic verification (such as verifying a date of birth) of identification information contained in an identity credential against a particular government record. The DVS is one of the identity verification services that operates via the DVS hub, which is one of the approved identity verification facilities supported by the Bill.

114. ***DVS document*** sets out the classes of documents that can be used as part of the 1:1 matching services authorised by the Bill. These classes are any of the following:

- birth, death, marriage and change of name certificates issued by or on behalf of an authority of a State or Territory, for example, the Registry of Births, Deaths and Marriages in New South Wales
- concession cards issued under the *Social Security Act 1991*
- certificates signed by an officer or documents that evidence the granting of a visa under the *Migration Act 1958*
- Australian citizenship certificates or notices given under section 37 of the *Australian Citizenship Act 2007*, as well as documents known as 'ImmiCards' that are issued to certain visa holders who are not an Australian citizen and do not hold a passport recognised by the Australian Government
- driver's licences and 'proof of age' cards issued by or on behalf of an authority of a State or Territory
- a document issued by a court setting out a divorce order made under the *Family Law Act 1975*
- an Australian travel document within the meaning of the *Australian Passports Act 2005*
- entry in a Roll within the meaning of the *Commonwealth Electoral Act 1918*
- either an aviation security identification card issued under the *Aviation Transport Security Act 2004* or a maritime security identification card issued under the *Maritime Transport and Offshore Facilities Security Act 2003*
- a medicare card within the meaning of subsection 84(1) of the *National Health Act 1953*.

115. The ***DVS hub*** means a facility developed, operated and maintained by the Secretary that is used for relaying electronic communications made in the course of requesting and providing DVSs. The DVS hub operates as a router by which requesting entities may request services, via the

Department, from agencies holding data. The agencies holding the data respond to requests via a return through the DVS hub. The DVS hub is one of the three approved identity verification facilities that the Secretary is authorised to develop, operate and maintain under Part 2 of the Bill.

116. ***DVS information*** has the meaning given by subclause 6(3) of the Bill. DVS information is information about an individual that is not facial images or biometric information, that falls into one of three categories.

- The first category is information about an individual that is contained in a document (the specimen document) that relates to the individual and purports to be a DVS document of a particular kind, and helps indicate whether the specimen document is a DVS document of that kind. This is intended to capture biographic information such as the name, date of birth, and address on the DVS document.
- The second category is information about an information that 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 document is a DVS document of that kind. This is intended to capture information on the DVS document which can be relied upon to determine whether the document is a DVS document, including driver licence numbers and Australian Passport numbers.
- The third category is information about the outcome of a comparison involved in a DVS relating to the person. This clarifies that the outcome of DVS request is considered to be DVS information, for example, confirming whether identity verification was successful.

117. ***Electronic communication*** means a communication of information in the form of data, text or images via either guided electromagnetic energy (such as optical fibre cable), unguided electromagnetic energy (such as radio waves), or both by a telegraphic, telephonic or other like service within the meaning of section 51(v) of the Constitution. Under the Bill, requests for, and responses to requests for, identity verification services will be sent to and from the approved identity verification facilities via electronic communications.

118. ***Entrusted person*** is defined in subclause 30(4) of the Bill to mean:

- the Secretary of the Department
- APS employees (as defined in section 7 of the *Public Service Act 1999*) in the Department
- a person whose services are made available to the Department who is:
  - an employee of an Agency as defined in the *Public Service Act 1999*
  - or an officer or employee of a state or territory
  - an officer or employee of a government authority (defined in this clause to mean an authority of the Commonwealth, state or territory but <u>not</u> a local government authority)
  - an officer or employee of the government of a foreign country or an authority of a foreign country, or an officer or employee of a public international organisation as defined in section 70.1 of the *Criminal Code*
- a contractor engaged to provide services to the Department in connection with an approved identity verification facility (whether the contractor is engaged directly or as a subcontractor), and
- an officer or employee of such a contractor whose duties relate wholly or partly to an approved identity verification facility.

119. The ***Face Matching Services hub*** means a facility that that is for relaying electronic communications (as defined in this clause) between persons and bodies for the purposes of requesting

and providing identity verification services (as defined in this clause), and is developed, operated and maintained by the Secretary. The FMS hub operates as a router by which requesting entities may request services, via the Department, from agencies holding data. The agencies holding the data respond to requests via a return through the FMS hub. The FMS hub is one of the three approved identity verification facilities that the Secretary will be authorised to develop, operate and maintain under Part 2 of the Bill.

120. ***Face-matching service information*** is defined in subclause 6(2) of the Bill. The definition is exhaustive and explicitly defined in this subclause to provide certainty and avoid the need to refer to definitions contained in other Acts. The definition includes information about an individual such as name, current or former address, place of birth, date of birth, age, sex, gender identity and whether a person is alive or dead. The definition also includes information contained in certain identity documents, such as a driver's licence, passport or visa. It also includes a facial image or biometric template derived from such an image.

121. ***Facial image*** is defined to be a digital still image of an individual's face that may or may not include their shoulders. A facial image is one type information used by the FIS and the FVS.

122. ***FIS*** is defined by reference to clause 16 of the Bill. The FIS is a 1:many matching service that The FIS is a 1:many matching identity verification service that is used to match a facial image of a person against images of persons held in government records. The FIS is one of the identity verification services, operating via the FMS hub that is authorised by the Bill. It will only be able to be used for the purpose of protecting shielded persons. A note to this definition clarifies that FIS is short for Face Identification Service, a term that is used in the intergovernmental agreement.

123. ***FVS*** is defined in clause 19 of the Bill. The FVS is a 1:1 identity verification service, and is used both for the purposes of verifying identities and protecting the identities of shielded persons. The FVS one of the identity verification services, operating via the Face Matching Services hub that is supported by the Bill. A note to this definition clarifies that FVS is short for Face Verification Service, a term that is used in the intergovernmental agreement.

124. ***Government authority*** means an authority of the Commonwealth, a State or a Territory, other than a local government authority. Local government authorities are excluded from this definition as they are considered to be non-government entities for the purposes of the Bill.

125. ***Government identification document*** means a document or other thing issued on behalf of a government authority that contains identification information and can be used to identify an individual or pass an individual off as someone else.

126. ***Identification information*** is defined in subclause 6(1) of the Bill to mean face-matching service information and DVS information, both of which are separately defined in clause 6. This term defines the information that is involved in requests for, or the provision of, identity verification services under the Bill.

127. ***Identity verification service*** means a 1:1 matching service (the DVS and FVS) or a 1:many matching service (the FIS).

128. ***IGIS official*** is defined to mean the Inspector-General of Intelligence and Security (being the person appointed for the purposes of section 6 of the IGIS Act) or a member of staff referred to in subsection 32(1) of the IGIS Act. This definition is included for the purposes of clause 33, which provides an exception to the offence at clause 30 where an entrusted person is permitted to make a record of, access or disclose protected information to an IGIS official in certain circumstances.

129. ***Intergovernmental agreement*** means the *Intergovernmental Agreement on Identity Matching Services* agreed to on 5 October 2017 by the Commonwealth, the States, the Australian Capital Territory and the Northern Territory. The intergovernmental agreement is an agreement to promote the secure, automated and accountable exchange of identity information, with robust privacy safeguards, for purposes including (but not limited to) preventing identity crime, protective security and identity verification. The DVS, the FVS and the FIS are covered by the intergovernmental

agreement. A note to this clause clarifies that subclause 39(1) of the Bill requires the Secretary to publish the intergovernmental agreement on the Department's website.

130. The ***NDLFRS*** means a system that is developed, operated and maintained by the Secretary under Part 2 of the Bill and consists of two elements:

- a database of identification information that is contained in, or associated with, government identification documents issued by (or on behalf of) an authority of a state or territory and is supplied by (or on behalf of) the authority to the Department by electronic communication for inclusion in in the database, and
- and a system for biometric comparison of facial images with facial images that are in that database.

131. The primary purpose of the NDLFRS is to create an electronic centralised repository of State and Territory driver's licence information (including the individual's photo, date of birth and address) and information associated with driver's licences (for example, whether a licence has been reported as lost or stolen). The NDLFRS can access facial images in the repository, subject to the approval of the government authority responsible for the identity credential, to create biometric templates that are used for biometric comparison. A biometric template is a mathematical representation of a facial image that cannot be used to recreate the facial image. A biometric template is a type of face-matching service information that is used by the FVS and the FIS.

132. A note to this definition clarifies that NDLFRS is short for National Driver Licence Facial Recognition Solution, a term that is used in the intergovernmental agreement.

133. ***NDLFRS hosting agreement*** is defined in clause 13 of the Bill to be a written agreement between the Department (representing the Commonwealth) and each authority of a State or Territory who supplies or proposes to supply identification information to the Department for inclusion in a database the NDLFRS. The Bill sets out the minimum obligations that are to be included in an NDLFRS hosting agreement, which State and Territory authorities must be a party to in order to access and use the NDLFRS.

134. ***Non-government entity*** means a body, or person, other than:

- the Commonwealth, a state or a territory; and
- a government authority (as defined above).

135. This definition is required because non-government entities, including private sector organisations and local government authorities, can make requests for 1:1 matching through the DVS and the FVS if the requirements of the Bill are met. A note to the definition provides that local government bodies in Australia and authorities of New Zealand are non-government entities because they are not covered by the definition of government authorities.

136. ***Ombudsman official*** is defined to be the Commonwealth Ombudsman, the Deputy Commonwealth Ombudsman or a member of staff referred to in subsection 31(1) of the Ombudsman Act. The Commonwealth Ombudsman and the Deputy Commonwealth Ombudsman are appointed under subsection 4(1) of the Ombudsman Act. This definition is included for the purposes of clause 34 of the Bill, which provides an exception to the offence at clause 30 that permits entrusted persons to make a record of, access or disclose protected information to an Ombudsman official in certain circumstances.

137. ***Participation agreement*** is defined in clause 8 of the Bill. All entities accessing identity verification services will be required to be a party to a participation agreement in respect of the relevant service. The Bill sets out the privacy obligations and other requirements of parties to participation agreements at clauses 9, 10, 11 and 12.

138. ***Personal information*** has the same meaning as given in section 6 of the Privacy Act. Section 6 of the Privacy Act provides that 'personal information' is information or an opinion about

an identifiable individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

139. ***Privacy impact assessment*** has the same meaning as given in subsection 33D(3) of the Privacy Act, which provides that a privacy impact assessment is a written assessment of an activity or function that identifies the impact that the activity or function might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

140. ***Protected information*** is defined by reference to clause 30 of the Bill, in particular the meaning provided under subclause 30(4). Division 2 of the Bill establishes a range of provisions for when protected information can be recorded, accessed or disclosed by a current or former entrusted person.

141. ***Rules*** means rules made by the Minister under clause 44 of the Bill. The rules can prescribe matters required or permitted by this Bill, or necessary or convenient for carrying out or giving effect to the Bill. Rules made under clause 44 will be legislative instruments.

142. ***Secretary*** is defined to be the Secretary of the Department. Consistent with section 19A of the Acts Interpretation Act, this means the Department of State of the Commonwealth that is administered by the Minister or Ministers administering that provision in relation to the relevant matter, and that deals with that matter.

143. ***Shielded person*** means a person who:

- 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 (paragraph (a) of the Bill). Section 15K of the Crimes Act defines a corresponding assumed identity law to be a law of a State or Territory, or a provision or provisions of a law of a State or Territory, prescribed by the Crimes Regulations 2019[3]
- has been given authority to acquire or use an assumed identity under Part IAC of the Crimes Act or a corresponding assumed identity law
- has been given a witness identity protection certificate under Part IACA of the Crimes Act
- has been given a witness identity protection certificate under a corresponding witness identity protection law. Section 15M of the Crimes Act defines a corresponding witness identity protection law as a law of a State or Territory or a provision or provisions of a State or Territory prescribed by the Crimes Regulations 2019[4]
- is a participant as defined in the Witness Protection Act. Section 3 of the Witness Protection Act defines a participant as person included in the National Witness Protection Program and, unless the contrary intention appears, a former participant;

---

[3] Regulation 9 of the Crimes Regulations prescribes the *Law Enforcement and National Security (Assumed Identities) Act 2010* (NSW); *Crimes (Assumed Identities) Act 2004* (Vic); Part 6B of Chapter 3 of the *Crime and Corruption Act 2001* (Qld); Chapter 12 and Divisions 1 and 4 of Part 5 of Chapter 24 of the *Police Powers and Responsibilities Act 2000* (Qld); Part 3 of the *Criminal Investigation (Covert Powers) Act 2012* (WA); Part 3 of the *Criminal Investigation (Covert Operations) Act 2009* (SA); the *Police Powers (Assumed Identities) Act 2006* (Tas); *Crimes (Assumed Identities) Act 2009* (ACT); Part 3 of the *Police (Special Investigative and Other Powers) Act 2015* (NT)

[4] Regulation 11 of the Crimes Regulations prescribes Part IIAA and sections 161 and 162 of the *Evidence (Miscellaneous Provisions) Act 1958* (Vic), Division 5 of Part 2 of the *Evidence Act 1977* (Qld), Part 4 of the *Criminal Investigation (Covert Powers) Act 2012* (WA), Part 4 of the *Criminal Investigation (Covert Operations) Act 2009* (SA), the entirety of the *Witness (Identity Protection) Act 2006* (Tas), Part 2 of the *Crimes (Protection of Witness Identity) Act 2011* (ACT) and Part 4 of the *Police (Special Investigative and Other Powers) Act 2015* (NT).

- is or was on a State or Territory witness protection program in which a complementary witness protection program is in force). Section 3 of the Witness Protection Act defines a complementary witness protection law as any State or Territory law that provides for the protection of a witness and is declared under section 3AA to be a complementary witness protection law,[5] or
- is involved in administering a witness protection program under such a law, and have acquired an identity under that law.

Clause 6—Definitions relating to identification information

144. Subclause 6(1) defines ***identification information*** to mean face-matching service information (defined in subclause 6(2)) and DVS information (defined in subclause 6(3)). Information may fall within the definition of both face-matching service information and DVS information. This does not preclude that type of information from being identification information.

145. The purpose of defining this term in this way is threefold. Firstly, to define the types of personal information which the Bill authorises the Department to collect, use and disclose. Secondly, to distinguish that information from other forms of personal information which it is not necessary for the Department to collect, use or disclose in providing the identity verification services. Thirdly, to distinguish those types of identification information which only needs to be collected, used or disclosed by the Department via the DVS and not the FVS nor the FIS.

146. ***Face-matching service information*** is defined in subclause 6(2) of the Bill. Paragraphs (a) to (q) of this subclause exhaustively outline the different types of information that constitute face-matching service information. These types of information are:

- a name by which the individual is or has been known (paragraph (a))
- a current or former address or the place or date the individual was born (paragraphs (b) and (c))
- an individual's age, current or former sex, gender identity or intersex status (paragraphs (d) and (e))
- information about whether an individual is alive or dead (paragraph (f))
- information contained in or otherwise associated with a driver's licence (however described) issued by a State or Territory (paragraph (g))
- information that is contained in or otherwise associated with a 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 providing the individual's identity (paragraph (h))
- information contained in or otherwise associated with a document that has been issued to an individual, as a person who is not an Australian citizen, by the Department administered by the Minister administering the Migration Act, to assist the person to prove their identity (paragraph (i))
- information that is:
    - contained in an Australian travel document (within the meaning of the Australian Passports Act) issued in the name of an individual
    - otherwise associated with the Australian travel document issued by the Minister administering the Australian Passport Act or the Department administered by that Minister, or

[5] These are set out in the Witness Protection (Complementary Witness Protection Laws) Declaration 2021.

    - otherwise associated with the Australian travel document by a government authority such as the Australian Border Force (ABF) by which the travel document may be inspected or seized under a law of the Commonwealth or of a state or territory (paragraph (j))
- information contained in or otherwise associated with a foreign travel document (within the meaning of the *Foreign Passports (Law Enforcement and Security) Act 2005*), or information that is associated with that document by a government authority by which the travel document may be inspected or seized under a law of the Commonwealth a State or a Territory (paragraph (k))
- an individual's current or former citizenship (paragraph (l))
- information contained in or otherwise associated with an current or former application for Australian citizenship, information contained in or otherwise associated with a document issued by the Commonwealth to provide evidence that the individual is or was an Australian citizen (paragraph (m))
- information about a current or former visa or entry permit granted to an individual under the Migration Act (paragraph (n))
- information contained in or otherwise associated with a current or past visa or entry permit application made under the Migration Act (paragraph (o)). This includes information contained in or otherwise associated with a visa or entry permit that was granted under the Migration Act
- a facial image of the individual, a biometric template derived from that image or a result of biometric comparison involving that image (paragraph (p))
- information about the outcome of a comparison involved in an FVS request in relation to the individual (paragraph (q)). This information is specifically included as the outcome of the DVS or FVS about an individual may be a match or no match response, which is not captured elsewhere in the definition in this subclause.

147. ***DVS information*** is defined in subclause 6(3) of the Bill to be:

- information, excluding facial and biometric information, that is contained in a document that relates to the individual and purports to be a DVS document; or information that is or is reasonably expected to be associated with a DVS document issued by a government authority relating to the individual and that helps indicate whether the document is a DVS document.
- information about the outcome of a comparison involved in a DVS relating to the individual.

148. DVS information includes information such as an individual's name, date of birth and address. It does not include facial image or any biometric matching information of the individual. This is because the DVS does not use any of this information, and is not capable of performing any biometric matching.

149. The information listed in subclause 6(4) of the Bill is excluded from the definition of both face-matching service information and DVS information. This information is:

- information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a trade union, sexual orientation or practices, or criminal record (paragraph (a))
- health information about an individual (as defined in section 6FA of the Privacy Act) (paragraph (b)), and

- genetic information about an individual (paragraph (c)).

150. Subclause 6(4) of the Bill directly replicates a large part of the definition of 'sensitive information' in subsection 6(1) of the Privacy Act. This information is inappropriate or not relevant to the purpose of verifying a person's identity. It therefore cannot be disclosed or used for the purposes of the identity verification services.

151. Subclause 6(5) of the Bill would provide that if information as defined in subclauses 6(2) and 6(3), also matches the description of information in subclause 5(4), it is still DVS or face-matching service information so long as the information is not primarily of the kind described in subclause 6(4).

152. Two examples are given in clause 6:

- Example 1 states that 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 states that 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.

Subdivision B—Common provisions for definitions of identity verification services

Clause 7—Simplified outline of this Subdivision

153. This clause contains a simplified outline of Subdivision B of Division 2 of Part 1 of the Bill. The simplified outline is included to assist readers to understand the substantive provisions of the Bill. The outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of the Bill.

Clause 8—Definition of *participation agreement*

154. This clause defines participation agreement to mean a written agreement between the Department (representing the Commonwealth) and one or more other parties, that:

- deals with the requesting and provision of identity verification services of one or more kinds using identification information made available by the parties, and
- meets the requirements in sections 9, 10, 11 and 12 (which include privacy obligations and other limits and compliance requirements).

155. All entities accessing the identity verification services will be required to be a party to a participation agreement in respect of the relevant service. These requirements are set out in paragraph 15(1)(b) for the DVS, paragraph 19(a) for the FVS and paragraph 17(1)(a) for the FIS.

156. Parties to the agreement will include:

- the Department as the administrator and operator of the identity verification services on behalf of the Commonwealth; and
- non-government organisations and Commonwealth, State and Territory government agencies that wish to make requests for relevant services offered under the identity verification services.

157. Each participation agreement would set out the respective roles, rights and obligations to each party when participating in, and accessing and using, the identity verification services. It would also provide a framework to set minimum security standards, privacy obligations and reporting requirements for each party. Non-compliance with a participation agreement may cause parties to the agreement to have their use and access to the identity verification services suspended or terminated.

158. Participation agreements will support the administration and operation of the identity verification services, protect the security and privacy of identification information, and provide

additional transparency and oversight regarding the use and operation of the services. The Bill requires a number of key privacy safeguards and protections to be contained in the participation agreement.

159. Subclause 8(2) of the Bill provides that, to avoid doubt:

- an agreement may be a participation agreement whether it was made before, on or after the commencement of clause 8
- different participation agreements may be made between the Department and different other parties, and
- paragraph 8(1)(b) and clauses 9, 10, 11 and 12 do not limit the matters that a participation agreement may deal with.

160. Paragraph 8(2)(a) reflects that some agreements are already in place between the Commonwealth (as represented by the Department) and agencies in a number of states and territories. If such agreements meet the requirements set out in the Bill, including in clauses 9, 10, 11 and 12, then they can be participation agreements for the purposes of the Bill.

161. Paragraph 8(2)(b) gives the Department the capacity to enter into separate participation agreements with other Commonwealth authorities, states and territories, who will be given access to a broader range of identity verification services, and separate ones with private sector organisations and local government agencies, who will only be able to access the DVS and the FVS under the Bill.

162. Paragraph 8(2)(c) would allow a participation agreement to contain matters further than those outlined in the Act. For example, the participation agreement may also deal with matters relating to the management of freedom of information requests and decisions, dispute resolution and further detail about training standards.

163. Clause 39 of the Bill requires the Secretary to make participation agreements publicly available on the Department's website.

Clause 9—General privacy obligations of parties to participation agreement

164. Clause 9 sets out the general privacy obligations of parties to participation agreements.

Subclause 9(1)—Privacy laws applicable to parties to a participation agreement

165. Under subclause 9(1), a party to a participation agreement must:

- be subject to the Privacy Act
- be subject to a privacy law of a State or Territory, where that law is prescribed by the in the rules
- have agreed to comply with the Australian Privacy Principles, with any modifications of Australian Privacy Principles 7.8 and 12.2 (about laws of the Commonwealth) specified in the agreement, as if the entity were an 'APP entity' within the meaning in clause 6 of the Privacy Act
- the entity is a government authority prescribed by the Minister in rules, and
- 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 (NZ) (paragraph (e) of the Bill).

166. Paragraph 9(1)(a) applies to entities that are subject to the Privacy Act. In general terms, the Privacy Act applies to Ministers, Departments, a range of Commonwealth agencies and organisations that are not small businesses operators (entities with an annual turnover of less than $3,000,000) (see sections 6, 6C and 6D of the Privacy Act).

167. Paragraph 9(1)(b) refers to entities that are subject to a privacy law of a State or Territory, such as the privacy laws in place in New South Wales, Victoria, Queensland, the Northern Territory

and the Australian Capital Territory. The application of these laws vary, but generally includes state or territory agencies such as road authorities.

168. Paragraph 9(1)(c) refers to entities that agree to comply with the Australian Privacy Principles, with any necessary modifications of subclauses 7.8 and 12.2, as if the party were an APP entity. This would apply to any private sector organisations that are not covered by the Privacy Act (such as small business operators who fall outside the scope of that Act) and any state or territory agencies in jurisdictions that do not have privacy laws falling within the scope of subclause 9(1)(b).

169. Paragraph 9(1)(d) refers to government authorities prescribed by the rules for the purposes of the paragraph. This would allow Commonwealth government authorities that are exempt from the Privacy Act, such as the Australian Security Intelligence Organisation, Australian Secret Intelligence Service, Australian Signals Directorate and Office of National Intelligence, to be parties to participation agreements. If State or Territory government authorities were unable to meet the requirements of paragraph 9(1)(c) then this would also provide an avenue for them to become party to a participation agreement.

170. Government authorities who wished to be prescribed in rules for the purposes of this paragraph would need to demonstrate that they have appropriate privacy rules and safeguards in place. Government authorities that are prescribed in the rules for the purposes of paragraph 9(1)(d) would also be required to comply with the privacy obligations under the participation agreement, as outlined at subclause 9(2) and clause 10. Overseas government authorities could not be prescribed for the purposes of paragraph 9(1)(d), as the definition of government authority is limited to Commonwealth, State and Territory agencies.

171. Paragraph 9(1)(e) refers to agreements that deal only with the requesting of DVSs (as defined in clause 15) by, and provision of DVSs to, an authority of New Zealand or an person or body operating in New Zealand. Such authorities, persons or bodies would need to be subject to the *Privacy Act 1993* of New Zealand in order to access the DVS. This supports the arrangements currently in place with New Zealand, providing for the use of the DVS by New Zealand based entities and a reciprocal arrangement for Australian entities to use the similar New Zealand service. A note to subclause 9(1) states that a DVS is the only identity verification that will be available to a party in New Zealand covered by paragraph 9(1)(e).

Subclause 9(2)—What a participation agreement must provide for

172. Subclause 9(2) sets out the minimum privacy requirements that must be included in a participation agreements.

173. Subclause 9(2)(a) requires participation agreements to provide for privacy impact assessments of requesting identity verification services. Under this provision, an agreement may provide that an entity must have a privacy impact assessment done in respect of its requests for services, or that it must be covered by a privacy impact assessment completed for its class of entity (e.g. police services), before being able to make any requests. Clause 5 provides that ***privacy impact assessment*** has the same meaning as given in subsection 33D(3) of the Privacy Act, which provides that a privacy impact assessment is a written assessment of an activity or function that identifies the impact that the activity or function might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. The requirement to be covered by a privacy impact assessment (paragraph 9(2)(a)) reflects the IGA, particularly paragraph 5.4 and 9.9.

174. Subclause 9(2) requires participation agreements to provide for the obtaining of an individual's 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 a limited exception applies for a government agency (paragraph (b)).This requirement will apply to all parties to participation agreements, including government authorities, all private sector organisations and local government agencies.

175. The only exception to this requirement is set out in subclauses 9(2)(b)(i) and (ii) and applies to Commonwealth, state and territory authorities where the 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. This reflects that it may not always be possible for officers captured at subclause 17(1) to obtain consent when seeking to use the FVS or FIS to protect the identity of a shielded person or someone else associated with a shielded person. For example, there may be a need for an authority to use the FVS years after a person has obtained an assumed identity under Part IAC of the *Crimes Act 1914* in order to ensure their identity continues to be protected. In this instance, it may be impractical for the government agency to obtain the consent of the individual without compromising a law enforcement investigation or the safety of the person with the assumed identity.

176. Under subclause 9(2)(c), when obtaining consent as required under paragraph 9(2)(b), a party to the participation agreement must notify an individual about the matters listed in subclause 9(3). This ensures the individual is provided with detail about how their information will be used and is in a position to provide informed consent.

177. Subclause 9(2)(d) requires parties to a participation agreement to have arrangements for dealing with complaints by individuals whose identification information is held by the party. This requirement will ensure individuals have an appropriate avenue to pursue any complaints directly with the party to the participation, and is not intended to preclude any separate complaint mechanism an individual may have, including complaints under the Privacy Act or to an ombudsman.

178. Subclause 9(2)(e) requires parties to participation agreements will be required to notify the Department of any breaches of security relating to the identity verification services. This requirement will not apply to the Department itself, which will be a party to all participation agreements. The requirement for parties to participation agreements to report security breaches to the Department under paragraph 9(2)(e) will enable a holistic response to such breaches. It will allow the Department to take action to prevent identification information from being compromised and work with government and industry to prevent any such breaches from occurring in the future.

179. Nothing in subclause 9(2)(e) is intended to exclude the operation of any state or territory notification requirements. This includes, for example, the mandatory data breach (information security incident) requirements on Victorian agencies under the Victorian Protective Data Security Framework and Standards. The notifiable data breach scheme under Part IIIC of the Privacy Act will also apply to those agencies subject to the Privacy Act.

180. Subclause 9(2)(f) requires the Department to inform the Information Commissioner of a breach of security that is reported to the Department (as a result of subclause 9(2)(e)) and is a data breach that is reasonably likely to result in serious harm to an individual whose identification information is involved in the breach. This obligation is intended to align with, and be read in a manner consistent with, the notifiable data breach scheme under the Privacy Act.

181. As the administrator and operator of the identity verification services, the Department is responsible for maintaining the security of identification information on the system and is in the best position to determine whether a security breach amounts to a data breach. Where it is a data breach that is reasonably likely to result in serious harm to an individual, referral to the Information Commissioner is an important safeguard and privacy protection, and ensures the Information Commissioner can take action if required.

Subclause 9(3)—Notice to an individual when obtaining consent to collect, use and disclose their identification information

182. Under subclause 9(3), when seeking consent for the collection, use and disclosure of their identification information, a party to a participation agreement is required to notify an individual of:

- how the party seeking consent uses identity verification services and how any facial images collected by that party for the purpose of making a request for services will be used and disposed of (paragraphs (a) and (b))
- whether facial images will be retained and used for other purposes (paragraph (c))

- what legal obligations the party seeking to collect identification information has in relation to that collection, what rights an individual has and what the consequences of declining to give consent are (paragraphs (d), (e) and (f))
- where the individual can get information about making complaints relating to the collection, use and disclosure of their identification information (paragraph (g), noting that every party to a participation agreement is required to have arrangements for dealing with complaints (see subclause 9(2)(d)), and
- where the individual can get information about the operation and management of the approved identity verification services (paragraph (h)). The information available on the Department's website for identity verification services (https://www.idmatch.gov.au) provides such information.

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

183. This clause sets out additional requirements for a participation agreement that specifically relate to parties to the agreement who request identity verification services (defined in clause 5 to mean 1:1 matching services—the DVS and FVS—and 1:many matching services—the FIS). As identity verification services will only be provided to parties to a participation agreement, this means that the provisions in clause 10 must be complied with when making requests for any of the identity verification services.

184. Subclause 10(1)(a) provides that parties to a participation agreement must only:

- request a DVS or FVS for the purposes of verifying the identity of an individual (subclause (a)(i)), or
- request a FVS or FIS for the purposes of protecting a shielded person or someone else associated with such a person (paragraph (a)(ii)).

185. This limits the purposes for which such services may be requested, in line with the objects of the Bill set out in clause 3. It ensures that the identity verification services cannot be used for other purposes, such as intelligence gathering, law enforcement activity or other community safety initiatives. This is an important safeguard and ensures that the use of the identity verification services is not authorised and is therefore prohibited.

186. Subclause 10(1)(b) provides that parties to participation agreements must comply with access policies which sets out additional conditions or standards that must be met by requesting agencies in order to access an identity verification services. Under clause 14, access policies for each service will set out the conditions that must be complied with in order for parties to access the services. These policies will be approved by the Coordination Group provided for in the intergovernmental agreement. Clause 39 requires the Secretary to publish the access policies on the Department's website.

187. Subclause 10(1)(c) of the Bill provides that the outcome of an identity verification service is not to be used as the sole evidence of an individual's identity in a criminal or civil proceeding. This reflects that the objects of the Bill are to enable identity verification. This supports access to industry and government services, and the digital economy. The Bill also aims to protect the safety of persons with an assumed identity and their associates. It is not intended that the identity verification services are used to conclusively prove a person's identity in criminal or civil proceedings.

188. Subclause 10(2)(a) provides that a participation agreement providing for a party to request identity verification services must provide for each party to the agreement not to disclose identification received by the party as a result of an identity verification service, subject to limited exceptions. These exceptions apply where the party is:

- required by law to disclose the results (for example, under a subpoena or freedom of information laws) (subclause (a)(i)); or

- permitted by law to disclose the results in circumstances specified in, or identified in accordance with, the participation agreement (subclause (a)(ii)) (for example with the consent of the relevant individual).

189. Subclause 10(2)(b) will require parties to the participation agreement who are Commonwealth, State and Territory government agencies to not permit an individual who is an officer, staff member, employee or contractor of that agency to receive any facial images by way of a response to an identity verification service or deal with a facial image provided in response to such a request unless the individual has been trained in facial recognition and image comparison. This is an important measure and ensures officers are appropriately trained in facial recognition and image comparison before they use the FVS or FIS to protect the identity of a shielded person or an associated person (see subclause 17(2)). It is proposed that the participation agreement will provide further detail about training requirements and standards for the purposes of paragraph 10(2)(b).

190. The obligation in paragraph 10(2)(b) does not extend to local government authorities or private sector organisations as they are not permitted to receive facial images in response to a request for the DVS or the FVS (being the only services they are permitted to access). The DVS does not involve any collection of facial images (see clause 6 and clause 15) and the FVS does not provide for the provision of any facial images to these entities (see subclause 19(d)).

191. A note is provided at the end of subsection 10(2) to clarify that non-government entities do not have access to facial images through the identity verification services.

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

192. This clause provides that 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 a service) to be able to limit the use of that information.

193. Clause 11 of the Bill implements the principle set out in clause 2.1(c) of the intergovernmental agreement, which provides that data providers to the identity verification services will retain control over which other agencies have access to information they hold, which are to be reflected in formal arrangements set out between agencies. These formal arrangements are set out in participation agreements and access policies.

194. This provision would allow, for example, a State or Territory that has provided driver licence data to the NDLFRS to limit how that information may be used. This will provide, for example, a mechanism by which use of the Australian Capital Territory's driver licence can be limited in accordance with the more limited terms under which the ACT entered into the intergovernmental agreement.

Clause 12—Requirements relating to compliance with participation agreement

195. This clause provides that each participation agreement must provide for annual auditing of compliance with the agreement, for each party to the agreement (except the Department) to report annually to the Department on the party's compliance with the agreement, and for the 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 or the access policies for a particular identity verification service.

196. The annual audit under subclause 12(a) and the requirement to report to the Department under subclause 12(b) are important safeguards and ensures the Department can monitor compliance with a participation agreement and, in particular, the requirements at clauses 9 (general privacy obligations), 10 (extra privacy obligations for parties to participation agreements who request services) and 14 (access policies for services). The Department will provide ongoing guidance to parties to support the annual auditing and compliance reporting.

197. The annual audit and compliance reporting will support the Department's annual reporting requirements at clause 41 and ongoing administration of the identity verification services, including

identifying whether any additional matters need to be included in the access policies. They may also support the annual assessment to be conducted by the Information Commissioner under clause 40.

198. Suspension or termination of a party to access the identity verification services under paragraph 12(c) of the Bill would provide the Department with the power to suspend or terminate access for parties that do not comply with terms of participation agreements. Suspensions and terminations must be reported on annually under paragraph 28(1)(k).

199. Suspension or termination of access is a powerful remedy in response to breaches of participation agreements or access policies. Suspension or termination would have significant consequences, including financial and reputational damage, given that use of the identity verification services is critical to industry and providing services to customers. While the Bill does not provide civil penalties for non-compliance with a participation agreement, the potential impact of a suspension or termination may be severe and is expected to act as a deterrent against non-compliance.

200. In practice, the annual audit (subclause 12(a)) and compliance reporting requirements (subclause 12(b)) may identity breaches of participation agreements and access policies and may trigger the Department to consider whether the party's ability to request identity verification services should be suspended or terminated.

Clause 13—NDLFRS hosting agreement

201. This clause provides for the NDLFRS hosting agreement, which is a written agreement between the Department (representing the Commonwealth) and each authority of a State or Territory that supplies or proposes to supply identification information to the Department for inclusion in a database in the NDLFRS. This agreement must:

- deal with the NDLFRS and the collection, use and disclosure of identification information in the NDLFRS (paragraph (1)(b)); and
- meet the requirements in subclauses 13(3), 13(4) and 13(5) (paragraph (1)(c)).

202. All states and territories that upload, or intend to upload, driver licence data to the NDLFRS are required to be a party to the NDLFRS hosting agreement. It follows that the required characteristics of the NDLFRS hosting agreement will apply to the Department and to each State and Territory party to the agreement.

203. Clause 39 requires the Secretary to make the NDLFRS hosting agreement publicly available on the Department's website.

Subclause 13(2)—State and Territory parties must be subject to privacy obligations

204. Under this subclause, each authority of a State or Territory that is party to the NDLFRS hosting agreement must:

- be subject to a privacy law of a State or Territory that is prescribed in rules for the purpose of subparagraph 13(2)(a)(ii), or
- be one of the following to which the Privacy Act applies
    - a state or territory authority (as defined in the Privacy Act), or
    - an instrumentality of a state or territory, or
- agree in the NDLFRS hosting agreement to comply with the Australian Privacy Principles, with any modifications of Australian Privacy Principle subclauses 7.8 and 12.2 (about laws of the Commonwealth) specified in the agreement, as if the entity were an 'APP entity'.

205. A note to this subclause clarifies that the Department, as the other party to the NDLFRS hosting agreement, is already subject to the Privacy Act.

206. By imposing this eligibility requirement, subclause 13(2) of the Bill ensures that each party to the NDLFRS hosting agreement is either subject to a privacy law, or agrees to be bound by privacy obligations. Importantly, this means that the parties have obligations with respect to collection, use and disclosure of personal information, and in relation to access to and correct of such information, that apply to each party to the agreement.

Subclause 13(3)—Requirements on each State or Territory party

207. Under this subclause, the NDLFRS hosting agreement must provide for each party to the agreement that is a State or Territory authority 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 (paragraph (a))
- provide each individual whose identification information is included in a database in the NDLFRS with a means of finding out what that information is and having any errors in that information corrected (paragraph (b))
- inform each such individual and the Department of any data breaches that involve identification information about the individual and the NDLFRS and are reasonably likely to result in serious harm to the individual (paragraph (c))
- provide means for dealing with complaints by individuals relating to the NDLFRS and identification information about them that is included in a database in the NDLFRS (paragraph (d)), and
- report annually to the Department on the party's compliance with the agreement (paragraph (e)).

208. There are three policy objectives that underpin this subclause. The first objective is to ensure that State and Territory parties are subject to accountability and oversight arrangements and encourage agencies to take compliance seriously.

209. The second objective is to provide a protective measure that ensures that individuals retain control over how their personal information is handled. For this purpose, it is important that individuals are provided with sufficient information on what personal information is held in the NDLFRS and how they can access, correct or make complaints about that information.

210. What is considered to be reasonable steps to notify an individual about the inclusion of their identification information, for the purposes of paragraph 13(3)(a) of the Bill, should be interpreted consistently with the notification requirements in Australian Privcy Principle 5 and the Australian Privacy Principles Guidelines available on the OAIC website.[6]

211. The third objective is to minimise harm in the event of a data breach, so that individuals and the Department have full knowledge of the nature of the personal information involved in the breach, the scope of the breach, and the particular risks of harm flowing from the breach. This will enable Department to take appropriate action including by reporting the data breach to the Information Commissioner in accordance with the Notifiable Data Breach Scheme under the Privacy Act.

212. The information received by the Department under subclause 13(3)(e) will be used in preparing the annual report required under clause 28.

[6] See https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information.

Subclause 13(4)—Requirements on the Department

213. Under this subclause, the NDLFRS hosting agreement must provide that the Department is required to:

- maintain the security of identification information included in a database in the NDLFRS, including by encrypting the information (paragraph (a))
- inform the other parties to the agreement of any data breaches involving that information and the NDLFRS (paragraph (b)), and
- inform the Information Commissioner of any data breaches that involve information and the NDLFRS, and are reasonably likely to result in serious harm to an individual to whom that information relates (paragraph (c)).

214. Subclause 13(4)(a) requires the Department to maintain the security of identification information included in a database in the NDLFRS. This requirement applies to the information held in the database itself, in contrast to the obligation placed on the Department in clause 25, which requires the Department to protect maintain the security of the electronic communications going to and from the approved identity verification facilities. In combination, these two provisions ensure the totality of the information and services provided by the Department are secured and encrypted.

215. The Department's obligation to maintain the security of identification information in subclause 13(4)(a) of the Bill is intended to be read consistently with, and supplement, the Department's obligations under Australian Privacy Principle 11. Under Australian Privacy Principle 11.1, the Department is required to take reasonable steps to protect personal information from misuse, interference and loss and from unauthorised access, modification or disclosure. This obligation is supplemented by the offence provisions established under Part 4 of the Bill, which operate to provide that identification information in a database in the NDLFRS must not be accessed or disclosed except where permitted under Division 3 of Part 4.

216. Subclause 13(4)(a) of the Bill does not prescribe a particular type of encryption. Decisions about how to implement the encryption required by this item will be a matter for the Department to determine in light of all the circumstances including, in particular, the technical configuration of the system or systems and whether a particular method or set of methods of encryption will be adequate to protect the security of the identification information on the NDLFRS This would also provide flexibility and ensures that any security measures align with contemporary cyber security standards.

217. The encryption requirements under paragraph 13(4)(a) should provide the Australian community with confidence that their identification information stored on the NDLFRS will be protected to the highest level possible. This requirement is similar to the requirement at paragraph 15(1)(a) of the Bill, to encrypt electronic information flows in the identity verification services.

218. Subclause 13(4)(b) requires the Department to inform the other parties to the agreement of any data breaches involving that information and the NDLFRS. This ensures that State or Territory authorities are alerted to such breaches and can fulfil their obligation to inform affected individuals of the breach, as required under subclause 13(3)(c), if the breach is reasonably likely to result in serious harm to the individual.

219. As the administrator and operator of the NDLFRS, the Department is responsible for maintaining the security of identification information on the system. Where it is a data breach that is reasonably likely to result in serious harm to an individual, referral to the Information Commissioner is an important safeguards and privacy protection, and ensures the Information Commissioner can take action if required.

220. The Department's obligation to notify the Information Commissioner under subclause 13(4)(c) is intended to align with, and be read in a manner consistent with, the notifiable data breach scheme under Part IIIC of the Privacy Act.

Subclause 13(5)—Requirement relating to compliance

221. Under this subclause, the NDLFRS hosting agreement must provide for suspension and 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. This is an important mechanism that will allow the Department to ensure compliance with the terms of the agreement and operate the NDLFRS in a manner consistent with the legislative requirements in this clause.

Subclause 13(6)—Timing and nature of agreement

222. This subclause would provide that:

- an agreement may be an NDLFRS hosting agreement whether it was made before, on or after the commencement of clause 13 of the Bill (paragraph (a)); and
- paragraph 13(1)(c) and subclauses 13(3), 13(4) and 13(5) do not limit the matters an NDLFRS agreement may deal with (paragraph (b)).

223. Paragraph 13(6)(a) of the Bill is important to include because an NDLFRS hosting agreement between the Commonwealth (as represented by the Department) and a number of States is already in place. That agreement will be amended prior to the commencement of the Bill to ensure that all legislative requirements in the Bill are captured.

224. Paragraph 13(6)(b) of the Bill would allow an NDLFRS hosting agreement to contain matters further than those outlined in the Act. For example, the NDLFRS hosting agreement may also deal with matters relating to the management of freedom of information requests and decisions, dispute resolution and further detail about the required security measures for identification information.

Clause 14—Access policies for services

225. This clause defines the term ***access policy***. Separate access policies will be developed for each of the identity verification services. The access policy for each service is the conditions that:

- must be complied with by parties to participation agreements for parties to have access (on request by the parties) of services of that kind (paragraph(a))
- are set out in a document approved by the Coordination Group provided for by the intergovernmental agreement (paragraph (b)), and
- 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 (paragraph (c)).

226. Subclause 14(a) of the Bill is supplemented by the operation of paragraph 10(1)(c), under which a party to a participation agreement that proposes to request identity verification services will be required to comply with the access policy for each service they request.

227. For the purposes of subclause 14(b), the Coordination Group will include officials from relevant Commonwealth, State and Territory agencies that are responsible for identity policy.

228. Access policies are intended to give flexibility to the Department (as the administrators of the identity verification services) to set contemporary standards to protect the security of the identity verification services, ensure they are only used for appropriate purposes, and protect the privacy of individuals. For example, the Department may require parties to a participation agreement to comply with certain security standards established by the Australian Government Information Security Manual and the Australian Signals Directorate's Essential Eight Maturity Model.

229. A note to clause 14 clarifies that under clause 39 of the Bill, the Secretary will be required to publish documents setting out access policies on the Department's website.

Subdivision C—Definition of DVS

Clause 15—Definition of *DVS*

230. This clause defines the DVS, which is an identity verification service that does not involve the collection, use or disclosure of any facial images or biometric templates. The DVS is a 1:1 matching service.

231. Under subclause 15(1), a service is a ***DVS*** if it meets all of the conditions set out in subclauses 15(1)(a) to (h). These are that:

- the service is, or is sought to be, provided on a request made by or on behalf of an authority, person or body (known as the ***requesting party***) (paragraph (a))
- the requesting party is a party to a participation agreement, as defined in clause 8 (paragraph (b))
- the request for the service includes DVS information that relates to an individual (other than information described in paragraph 6(3)(b), which defines DVS information and relates to information about the outcome of a comparison involved in a DVS relating to the individual) and to a specimen document purporting to be a DVS document that:
    - is of a kind specified in a request, and
    - is issued by a government authority that is or was responsible for the issue of DVS documents of that kind (paragraph (c))
- the service involves, or is to involve, an electronic comparison of that DVS information and information that:
    - is contained in with, DVS documents of the kind specified in the request, or is associated with such documents by the government authority that is responsible for issuing them (referred to as the issuing authority in this clause) and is a party to a participation agreement, and
    - is made available for the comparison by the issuing authority (paragraph (d))
- the comparison is carried out in accordance with any limitations that the issuing authority has provided for in the participation agreement in which the issuing authority agreed to make the information available for the comparison (which is possible under clause 11) (paragraph (e))
- the purpose of the comparison is to help to determine whether the specimen document, as described in paragraph 15(1)(c), is a DVS document of the kind specified in the request (paragraph (f))
- the response to the requesting party about the outcome of the comparison is limited to either a statement that the information compared did match, a statement that the information did not match, with or without reasons as to why the information did not (paragraph (g)), and
- the request and the response to the request are communicated by electronic communications relayed through the DVS hub or the Face Matching Services hub, as defined in clause 5 (paragraph (h)).

232. For example, these requirements would be satisfied in the following scenario.

- A bank is a party to a participation agreement and, as part of their standard customer identification procedures, seeks to verify the identity of a new customer who wishes to open an account. The customer elects to provide their driver's licence to the bank to enable the verification of their identity.

- The bank (in this case, the requesting party) makes a DVS request by filling out a form on an online interface with DVS information from the licence (such as the name, date of birth and licence number), and the type of DVS document (a driver's licence).
- The request is communicated electronically through the DVS hub to the data hosting agency, in this case the state or territory road authority that issued the licence. The DVS information provided on the DVS request is compared against the identification information on the state or territory road authority's database. This means that the verification of the customer's identity occurs within the road authority's database or infrastructure.
- Should there be a successful match, the outcome of the DVS request is electronically communicated to the bank via the DVS Hub.

233. Clause 15(1)(b) of the Bill is an important mechanism by which the privacy and accountability safeguards that will apply to an entity under a participation agreement, as outlined in Subdivision C of Division 2 of Part 1, will apply to any entity using the DVS hub for a DVS.

234. Paragraphs 15(1)(c) and (d) of the Bill make clear that only information in, or associated with, a DVS document will be used in performing a DVS. This information does not include a facial image or biometric templates.

235. The response to a request for a DVS is, in all instances, limited to 'match or no match' under paragraph 15(1)(g) of the Bill. Information that can be provided with a 'no match' response includes an indication of the reasons why the information did not match.

236. Note 1 to subclause 15(1) clarifies that DVS is short for Document Verification Service, which is a term used in the intergovernmental agreement.

237. Note 2 to subclause 15(1) states that DVS is an example of a 1:1 matching service, which is defined in section 5.

238. Subclause 15(2) of the Bill provides that the requirements for the requesting party and the document issuing body to be parties to a participation agreement do not apply in relation to a service requested within 12 months after the commencement of clause 15. In accordance with clause 2, clause 15 will commence on the day after Royal Assent.

239. The DVS is a longstanding service which is currently used by over 2,700 government agencies and private sector organisations, matching against documents provided by more than 20 government agencies. These entities are party to memoranda of understanding (for government agencies) or contractual arrangements (for business users) outlining the terms of their participation of the services. Subclause 15(2) of the Bill is intended to provide the Department with sufficient time to make amendments to these documents so that they meet the requirements of a participation agreement under this legislation, without disrupting the operation of the service.

Subdivision D—Definition of FIS

Clause 16—Definition of *FIS*

240. This clause defines the FIS, which is an identity verification service that does not involve the collection, use or disclosure of any facial images or biometric templates. The FIS is a 1:many matching service.

241. Under this clause, a service would be a FIS where it meets four requirements, namely where:

- the service is, or is sought to be, provided on a request (paragraph (a) of the Bill);
- the requirements of clause 17 are met in relation to the request (paragraph (b));
- the service involves, or is to involve, a comparison that has the characteristics and purpose set out in clause 18 (paragraph (c)); and

- the request and the outcome of the comparison are communicated by electronic communications related through the Face Matching Services hub (paragraph (d)).

242. The FIS is a 1:many matching service that can only be used by officers from a limited group of Commonwealth, State and Territory agencies when authorised to do so for the purpose of protecting the identity of shielded persons and their associates. Shielded persons are defined in clause 5 and, generally speaking, include those persons who have been authorised to acquire or use an assumed identity (for example, an undercover police officer) under law, including the Crimes Act and Witness Protection Act. The FIS cannot be used for any other purposes, including other purposes listed in the IGA.

Clause 17—Requirements for valid request for FIS

243. This clause would provide that the following requirements must be met in order for a FIS request to be valid:

- the request for a FIS must be made by an officer on behalf of one of the Commonwealth, State or Territory government authorities listed in paragraph 17(1) that is a party to a participation agreement, for the purpose of protecting the identity of a shielded person or someone else associated with a shielded person (subclause 17(1)(b))
- the person making the request for a FIS 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) (subclause 17(2))
- the request must have specific characteristics and include a single facial image of an individual (subclause 17(3))
- the request for a FIS must be endorsed by a senior officer of the same government authority, by electronic communication to the Face Matching Service hub (subclause 17(4)), and
- a person must not endorse a request made on behalf of an authority unless satisfied that the request is made for the purposes of protecting a shielded person, or associate, stated in the request, and the performance of the authority's functions (subclause 17(5)).

Subclause 17(1)—Requesting authorities

244. Subclause 17(1)(a) provides that a request for a FIS must only be made by any of the following officers of a Commonwealth, state or territory government authority that is a party to a participation agreement:

- a law enforcement officer or intelligence officer within the meaning of section 15K of the Crimes Act;
- an officer (however described) of an agency authorised under a corresponding assumed identity law within the meaning of section 15K of the Crimes Act; and
- an officer of an approved authority in line with the powers and functions of the agency as a participant in the National Witness Protection Program under the *Witness Protection Act 1994* or as a participant in a witness protection program under a complementary witness protection law declared under section 3AA of that Act .

245. The intent of subclause 17(1)(b) is to clarify that officers of the approved agencies listed at subclause 17(1)(a) are the only persons authorised to make a request for a FIS. Unlike the 1:1 matching services, the FIS will not be able to be accessed by other government authorities, local government authorities or private sector organisations. This is appropriate given that a FIS may only be requested for the purpose of protecting shielded persons, as defined in clause 5

246. The listed agencies can only gain access to the FIS and make a request if they are a party to a current participation agreement. The agency that protects shielded persons and those associated with

shielded persons is the party that can make the request (upon entering into the relevant participation agreement), not the department administering the relevant legislation.

247. Subclause 17(1)(b) provides that a request for a FIS can only be made 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 (as defined in clause 5).

248. The FIS is a critical tool to protecting shielded persons. For example, a FIS request may be submitted in regards to an officer from a law enforcement agency who will be going undercover to infiltrate a criminal organisation and, accordingly, has been authorised to acquire an assumed identity under Part IAC of the Crimes Act. In this instance, the FIS request will allow for the officer's digital photo to be searched across data holding agencies to determine if the undercover officer has a government identification document (like a licence or passport) under their true identity or a different identity which may have been used in a previous undercover operation.

249. If a match has been identified, the relevant law enforcement agency will be able to work with relevant agencies to ensure the government identification document for the undercover officer is not accessible for identity verification purposes via a DVS or FVS search.

250. Without this capability, the identity of an undercover officer could be compromised by the criminal organisation. This could compromise an active investigation and undermine the safety of the undercover officer and their family.

Subclause 17(2)—Person making request

251. This subclause would require the person who is requesting a FIS to on behalf of an authority to be approved as a suitable person to make a request. A person may be approved to as a suitable person to make requests for a FIS by:

- the head (however described) of the Commonwealth, state or territory authority that the person works for (paragraph(a)), or
- a person who is:
    - the holder of a management office or position in the authority
    - is authorised, by notice in writing to the Department, by the head of the authority to approve persons to make requests for a FIS, and
    - is senior to the person making the request (paragraph (b)).

252. A note to subclause 17(2) clarifies that the relevant Commonwealth, state or territory authority (that meets the requirements in subclause 17(1)) would have obligations under the participation agreement to only approve a person to request access to the FIS where that person has completed training in facial recognition and image comparison (see paragraph 10(2)(b)). Training in facial recognition and image comparison will help to ensure that protective measures for shielded persons will be applied to the correct identity credentials.

253. Each authority would also have an obligation to provide the Department with copies of any authorisation given by a head of an authority for a person in a management office or position in the authority to approve persons to request a FIS (subclause 17(2)(b)(ii)). This ensures the Department has a record of approved requesting officers and can build these safeguards into the system.

Subclause 17(3)—Request stating relevant activity

254. This subclause outlines requirements in relation to the request for a FIS for the purposes of subclause 16(b) of the Bill. A request for a FIS must:

- include a single facial image of an individual, and may contain other face-matching service information about the individual (paragraph (a)), and
- specify the kinds of government identification documents against which the face-matching service information in the request is to be compared (paragraph (b)), partly by

reference to whether the documents issued is by or on behalf of an authority of the Commonwealth, or a specified State or Territory (paragraphs (b)(i)-(iii)).

255. The requirements listed in subclause 17(3) of the Bill would be incorporated into the FIS interface for the Face Matching Services hub, meaning that an individual approved to use the FIS under subclause 17(2) would only be able to request a FIS where all of this information is provided. The FIS interface for the FMS hub is provided by the Department.

256. Subclause 17(3)(a) of the Bill is an important privacy safeguard in the Bill, as it provides that a request for an FIS may only include a single facial image. In other words, an automated stream of images cannot be fed into the FIS and a specific request about a specific image will need to be made.

257. Paragraph 17(3)(b) of the Bill would have the effect of requiring that a request for a FIS list the particular type(s) of government identification document(s) that the FIS would search, including by reference to the jurisdiction under which that type of document was issued. For example, this means that a request for a FIS must nominate whether a driver licence issued by a State or Territory agency, an Australian passport, or a government identification documents issued by the Department (or a combination of these) is to be searched.

258. A note to subclause 17(3) advises that making a false or misleading statement in the request may be an offence against section 136.1 of the Criminal Code.

Subclauses 17(4) and (5)—Endorsement of request

259. Subclause 17(4) of the Bill requires that a request for a FIS must be endorsed prior to any FIS search is performed by electronic communication to the Face Matching Services Hub. This provision would mean that any request for a FIS is required to be reviewed and endorsed by a person who is:

- the head (however described) of the authority from which the request for a FIS originates , or
- a person who is:
    - the holder of a management office or position in the authority
    - is authorised, by notice in writing to the Department, by the head of the authority to approve persons to make requests for a FIS, and
    - is senior to the person making the request.

260. If a person is authorised by the head of their authority to endorse requests for a FIS, the authority is required to provide a copy of this written authorisation to the Department (under subparagraph 17(4)(a)(ii)). This ensures the Department has a record of approved requesting officers and can build these safeguards into the system.

261. Subclause 17(4)(b) requires that the request must be made by electronic communication to the Face Matching Service Hub, as defined in clause 4. Consistent with clause 25, the Department must maintain the security of electronic communications to and from the facility, including by encrypting the information.

262. A note to subclause 17(4) of the Bill provides that the endorsement of a request for a FIS may occur at the time of, or shortly after, the request. This reflects the operation of the FIS interface. Once a request for a FIS is entered by an officer who is approved under subclause 17(2), an automatic notification will be generated for an endorsing senior officer who is authorised under subclause 17(4)(b). That endorsing senior officer then needs to consider whether the request meets the requirements in subclause 17(5) before endorsing the request. The FIS search will only be performed after the endorsement has been received.

263. Subclause 17(5) of the Bill outlines the matters that an endorsing officer must be satisfied of before endorsing a request for the purposes of subclause 17(4). These matters are that the request must be made for the purposes of:

- protecting a shielded person or someone else associated with a shielded person, stated in the request; and
- the performance of the authority's functions.

264. If the endorsing officer is not satisfied that the request meets the requirements in subclause 17(5) of the Bill, they must not endorse the FIS request. Without an endorsement under subclause 17(4) and (5), a FIS search cannot be performed.

265. Subclause 17(5) of the Bill ensures that the 1:many matching functionality available through the FIS can only be used for the limited purpose of protecting shielded persons and their associates, in the performance of an appropriate authority's functions. This limitation ensures that the FIS cannot be used for broader intelligence, law enforcement or community safety purposes.

266. The annual report under clause 41 must include information on the number of times the FIS was used each financial year and whether the requests were endorsed as required by subclause 17(5).

Clause 18—Characteristics and purpose of comparison involved in FIS

267. This clause sets out the characteristics and purposes of any comparison conducted under the FIS.

268. Subclause 18(1) of the Bill sets out how a facial image of an individual, and any other face-matching service information, in the request for a FIS is electronically compared with face-matching service information.

269. A request for a FIS will include a single facial image of an individual and may include further face-matching service information about that individual (such as gender or age range). That information will be compared electronically with other face-matching information, including drivers licence information contained in the NDLFRS that:

- relates to one or more individuals
- is contained in, or associated with, one or more government identification documents or one or more kinds specified in the request, and
- is made available for the comparison by a government authority that is a party to a participation agreement.

270. Subclause 18(2) of the Bill provides that any comparison that is performed by the FIS would be carried out in accordance with the limitations provided for under the participation agreement, subject to which the supplying authority made the face-matching service information available for the comparison. This provision allows agencies who make their data available for comparison to maintain control over how their data is used.

271. Subclause 18(3) of the Bill provides that the purpose of protecting an individual who is a shielded person, or someone else associated with a shielded person. For example, a comparison in a FIS may be required for the purpose of identifying the individual, or determining whether the individual has multiple identities, for the purpose of ensuring that person's protection.

Subdivision E—Definition of FVS

Clause 19—Definition of *FVS*

272. This clause defines the FVS, which is service that will allow a participating government agency (including Commonwealth, State, Territory and local government agencies) or private sector organisation to verify an individual's known or claimed identity using a facial image of the person on a government identification document. The FVS is a 1:1 matching service

273. The FVS will provide different types of functionality depending on what entity is requesting the service. For example, a local government agency or private sector organisation is limited to receiving either a 'match' or 'no match' response (see paragraph 10(d)). To request an FVS, these entities will upload a facial image of an individual and any further face-matching service information (such as name and date of birth) they have about that individual. That image will be compared against facial images in government identification documents, such as driver's licences and passports, to provide the response. For Commonwealth, State and Territory agencies, the response may also include further face-matching service information about the individual such as the person's image on the government identification document, and further information on or associated with that document.

274. Clause 19 provides that a service is an FVS if:

- 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 is not a participation agreement that deals only with the requesting of DVSs by, and the provision of DVSs to, an authority or New Zealand or a person or body operating in New Zealand (paragraph(a))
- the request includes face-matching service information (as defined in subclause 6(2)) about an individual (paragraph (b))
- the service involves, or is to involve, a comparison that has the characteristics and purpose set out in clause 20 (paragraph (c))
- if the requesting entity is a non-government entity (i.e. a local government authority or private sector organisation)—the response to the comparison request is only a 'match' or 'no match' response and does not contain any other face-matching service information that relates to the individual (paragraph (d)), and
- the request and the response are communicated by electronic communications relayed through the Face Matching Services hub (paragraph (e)).

275. Subclause 19(a) of the Bill would operate to provide that the FVS cannot be provided to an authority of, or entity in, New Zealand. This is different to the DVS, which can be provided to New Zealand (as they fall within the definition of 'non-government entity' in clause 5). The FVS is solely being provided to Australian agencies and entities.

276. Subclause 19(a) of the Bill would also provide that any authority requesting an FVS is required to be a party to a participation agreement. This is an important mechanism by which the privacy protections and oversight requirements outlined in a participation agreement apply to any party requesting a FVS (see clauses 8 to 12).

277. Subclause 19(e) requires that the request must be made by electronic communication to the Face Matching Service Hub, as defined in clause 4. Consistent with clause 25, the Department must maintain the security of electronic communications to and from the facility, including by encrypting the information.

278. Note 1 to clause 19 clarifies that FVS is short for Face Verification Service, which is a term used in the intergovernmental agreement.

279. Note 2 to clause 19 states that the FVS is an example of a 1:1 matching service, as defined in clause 5.

Clause 20—Characteristics and purpose of comparison involved in FVS

280. Subclause 20(1) of the Bill outlines the comparison that is involved in an FVS. This comparison is an electronic comparison of:

- face-matching service information (including a facial image) about an individual that is included in the request for the service under subclause 19(b) (paragraph (a)), and
- face-matching service information that is contained in, or associated with, a government identification document of a kind specified in the request, where that document has been

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

281. Subclause 20(1)(b) of the Bill also provides that any Commonwealth, State or Territory agency that is making government identification documents available for comparison must be a party to a participation agreement. This is an important mechanism by which the privacy protections and oversight requirements outlined in a participation agreement apply to government agencies making data available for comparison via a FVS (see clauses 8 to 12).

282. Subclause 20(2) provides that the comparison involved in an FVS is carried out in accordance with any limitations provided for under the participation agreement, subject to which the supplying authority made the face-matching information available for the comparison.

283. Subclause 20(3) provides that the comparison involved in a FVS can only be for the purpose of either verifying the identity of the individual (paragraph (a)), or protecting an individual who is a shielded person or someone associated with that shielded person (paragraph (b))

Division 3—Miscellaneous

Clause 21—False and misleading statements in requests for services

284. Clause 21 makes it clear that a request for an identity verification service is an application for a benefit for the purposes of section 136.1 of the Criminal Code. A note to clause 21 clarifies that section 136.1 creates offences for making false or misleading statements in applications for benefits.

285. The effect of this is that any false or misleading statement made in a request for an identity verification service may be:

- an offence against subsection 136.1(1) of the Criminal Code where a person makes a statement in the request knowing that the statement is false or misleading, or omits a matter without which the statement is misleading; or
- an offence against subsection 136.1(4) of the *Criminal Code* where a person makes a statement in the request and is reckless to whether the statement is false or misleading, or omits any matter or thing without which the statement is misleading.

286. These offence provisions would be applicable in addition to any potential administrative sanctions that may be placed on an individual or an entity for improper use of the identity verification services including the suspension and termination of an entity's access to an identity verification service where they do not comply with the requirements of a participation agreement, or the NDLFRS hosting agreement (see clause 12 and subclause 13(5) of the Bill respectively).

Clause 22—This Act binds the Crown

287. This clause provides that the Bill would bind the Crown in each of its capacities. This provision is intended to ensure that all Commonwealth, State and Territory agencies (and their officers, employees etc) are bound by the requirements in the Bill.

Part 2—Developing and operating approved identity verification facilities

Clause 23—Simplified outline of this Part

288. This clause contains a simplified outline of Part 2 of the Bill.

289. The simplified outline is included to assist readers to understand the substantive provisions of the Bill. The outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of the Bill.

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

290. This clause provides authority for the Department to develop, operate and maintain the approved identity verification services. Clause 5 defines ***approved identity verification services*** to

mean the DVS hub, Face Matching Service Hub and NDLFRS, all of which are also separately defined in clause 5.

291. This provides authority for the Department to establish the information technology solutions for the approved identity verification services, operate them in accordance with the requirements of the Bill and maintain them on an ongoing basis.

292. Subclause 24(2) provides that the authorisation to operate the DVS hub in subclause 24(1) does not limit the ability of the Department to develop, operate and maintain the Face Matching Services hub (subclause (2)). This provides flexibility for the Department to establish these systems using the most appropriate and cost-effective information technology solutions. For example, the technological solution for the DVS hub and Face Matching Services Hub could be combined but they could still be maintained as separate identity verification facilities for the purposes of this Bill.

Clause 25—How facilities are to be developed, operated and maintained

293. This clause provides that, in developing, operating and maintaining an approved identity verification facility (as defined in clause 5), the Department must:

- maintain the security of electronic communications to and from the approved identity verification facilities, including by encrypting the information (paragraph (a)), and
- protect the information from unauthorised interference or unauthorised access (paragraph (b)).

294. The intention of subclause 25(a) is to require encryption to be used, as a minimum, when seeking to protect and maintain the security of information flows to and from the approved identity verification facilities. However, subclause 25(a) acknowledges that the Department may need to take additional steps and implement other security measures in order to protect information flows.

295. For example, in addition to using encryption, the Department may also need to implement access controls, firewalls and cyber security measures to protect the security of information flows. In practice, the Department will engage with government agencies like the Australian Signals Directorate, on an ongoing basis, and reflect on national and international best practice when implementing measures to maintain the security of information flows. The Department will also consult and engage with States and Territories, and industry on the implementation of additional security measures.

296. Clause 2 requires the Department to protect maintain the security of the electronic communications going to and from the approved identity verification facilities. This complements the requirement in subclause 13(4)(a) for the Department to maintain the security of identification information included in a database in the NDLFRS, which applies to the information held in the database itself. In combination, these two provisions ensure the totality of the information and services provided by the Department are secured and encrypted

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

Division 1—Simplified outline

Clause 26—Simplified outline of this Part

297. This clause contains a simplified outline of Part 3 of the Bill.

298. The simplified outline is included to assist readers to understand the substantive provisions of the Bill. The outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of the Bill.

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

Clause 27—Collection of identification information by the Department

299. Subclause 27(1) authorises the Department to collect identification information, whether or not the information is sensitive information as defined in the *Privacy Act 1988*, that relates to an

individual from someone other than the individual. The collection is only authorised if it is for a purpose listed in subclause 27(2) and is covered by one of the methods of collections listed in subclauses 27(3), 27(4) or 27(5).

300. For example, the Department may collect identification information (such as driver's licence data) from a state or territory road authority for the purpose of developing the NDLFRS as this is a purpose listed in paragraph 27(2)(d) of the Bill and a collection covered by paragraph 27(5).

301. A note to subclause 27(1) clarifies that one effect of this clause 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), which is about sensitive information, and subparagraph 3.6(a)(ii), which is about personal information.

302. Subclause 27(2) of the Bill provides that the purposes for which the Department may collect identification information:

- providing a DVS or FVS for the purpose of verifying the identity of an individual (paragraph (a))
- providing a FVS or FIS for the purpose of protecting a shielded person or someone else associated with a shielded person (paragraph (b))
- developing identity verification services, or facilities for providing those services for the purpose of providing a DVS or FVS for the purpose of verifying the identity of an individual or providing a FVS or FIS for the purpose of protecting a shielded person or someone else associated with a shielded person (paragraph (c)), or
- developing, operating or maintaining the NDLFRS (paragraph (d)).

303. Nothing in subclause 27(2) of the Bill is intended to limit the collection of identification information for more than one purpose listed in paragraphs 27(2)(a) to (d).

304. Subclauses 27(3), (4) and (5) support the authorisation for the Department to collect identification information under subclause 27(1). This authorisation will only apply if the collection is covered by one of the subclauses.

- Subclause 27(3) of the Bill covers the collection of information by means of an electronic communication to or from the DVS hub, for the purpose of making or responding to a request for a DVS.
- Subclause 27(4) of the Bill covers the collection of identification information by means of an electronic communication to the Face Matching Services hub that either requests the provision of an identity verification service (paragraph (a)), responds to such a request (paragraph (b)), or supplies the information to a database in the NDLFRS (paragraph (c)).
- Subclause 27(5) of the Bill covers the collection of information by means of an electronic communication to the NDLFRS. This can either be a request for information or the provision of information.

305. Subclause 27(6) makes it clear that subclauses 27(2) to (5) of the Bill are not intended to implicitly authorise the disclosure of identification information to the Department or affect the authorisation of the disclosure of information under other Commonwealth, state or territory provisions. This reflects that the Bill is intended only to authorise the Department to provide the identity verification services, and that in seeking to use or otherwise participate in the services, other organisations must have a separate legal authority or permission to disclose identification information to the Department.

Clause 28—Use and disclosure of identification information by the Department

306. Subclause 28(1) of the Bill authorises the Department to use or disclose identification information for any of the purposes listed in subclause 27(2), if the identification information is:

- collected by means of an electronic communication with an approved identity verification facility (paragraph (a)), or
- held in, or generated using, the NDLFRS (paragraph (b)).

307. Subclause 27(2) of the Bill provides that the purposes for which the Department may collect identification information:

- providing a DVS or FVS for the purpose of verifying the identity of an individual
- providing a FVS or FIS for the purpose of protecting a shielded person or someone else associated with a shielded person
- developing identity verification services, or facilities for providing those services for the purpose of providing a DVS or FVS for the purpose of verifying the identity of an individual or providing a FVS or FIS for the purpose of protecting a shielded person or someone else associated with a shielded person, or
- developing, operating or maintaining the NDLFRS.

308. A note to subclause 28(1) clarifies that one effect of the clause is that such use or disclosure of identification by the Department is authorised for the purposes of provisions of Australian Privacy Principle 6. such as paragraph 6.2(b), which relates to use or disclosure of personal information authorised by law.

309. Subclause 28(2) of the Bill clarifies that subclause 28(1) does not implicitly authorise a person or body to collect identification information disclosed by the Department under subclause 28(1) or 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. This reflects that the Bill is intended only to authorise the Department to provide the identity verification services, and that in seeking to use or otherwise participate in the services, other organisations must have a separate legal authority or permission to collect identification information.

Part 4—Protection of information

Division 1—Simplified outline

Clause 29—Simplified outline of this Part

310. This clause sets out a simplified outline of Part 4 of the Bill.

311. The simplified outline is included to assist readers to understand the substantive provisions of the Bill. The outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of the Bill.

Division 2—When protected information can be recorded or disclosed

Clause 30—Offences by entrusted persons

312. This clause creates two new criminal offences in relation to entrusted persons where they make a record of, disclose or access protected information. The clause also provides for exceptions to the offences in certain circumstances.

Offence for recording or disclosing information

313. Subclause 30(1) makes it an offence for a person who is, or has been, an entrusted person to make a record of or disclose protected information, where the person obtained the protected information. The offence would consist of the following physical elements:

- the person is, or has been, an entrusted person
- the person has obtained protected information in their capacity as an entrusted person, and
- the person makes a record of the information or discloses the information to another person.

314. The fault element for the first two physical elements in subclauses 30(1)(a) and (b) of the offence is recklessness. This is clarified in a note to subclause 30(1). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is aware of a substantial risk that the result will occur and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

315. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to the third physical element in subclause 30(1)(c). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

316. The terms ***entrusted person*** and ***protected information*** are defined in subclause 30(4).

317. The maximum penalty for the offence would be imprisonment for two years. The maximum penalty needs to be adequate to deter and punish a worst case offence, including repeat offences. This penalty is appropriate to reflect the serious consequences that may arise from the relevant conduct, given that breach of the obligations of entrusted persons may place a person's life or safety at risk.

Offence for accessing information

318. Subclause 30(2) makes it an offence for a person who is an entrusted person to access protected information. The offence would consist of the following physical elements:

- the person is an entrusted person, and
- the person accesses protected information.

319. The fault element for the first physical element in subclause 30(2)(a) is recklessness. This is clarified in a note to subclause 30(2). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is aware of a substantial risk that the result will occur and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk

320. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to the second physical element in subclause 30(2)(b). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct

321. The terms ***entrusted person*** and ***protected information*** are defined in subclause 30(4).

322. The maximum penalty for the offence would be imprisonment for two years. The maximum penalty needs to be adequate to deter and punish a worst case offence, including repeat offences. This penalty is appropriate to reflect the serious consequences that may arise from the relevant conduct, given that breach of the obligations of entrusted persons may place a person's life or safety at risk.

Exceptions

323. In addition to the general defences available under Part 2.3 of the Criminal Code, clause 30 creates specific exceptions to the offences set out in subclauses 30(1) and (2). These exceptions apply where:

- the conduct is authorised by a law of the Commonwealth or of a state or territory,
- the conduct is in compliance with a requirement under a law of the Commonwealth or of a state or territory.

324. The offences in subclauses 30(1) and (2) are only intended to apply where an entrusted person's conduct is not a proper or legitimate part of their work. There are a vast range of legitimate circumstances in which entrusted persons will need to access, make a record of, or disclose protected information in performing their duties. These exceptions will ensure that the Department is not prevented from performing its role in developing, maintaining or operating the identity verification services.

325. The new offences would make it clear that current and former entrusted persons must ensure that they only access, make a record of, or disclose protected information if they have appropriate authorisation under, or are acting in compliance with, a requirement of a Commonwealth, state or territory law, including conduct authorised by this Bill. This would also contribute to reducing the risk of harm to the safety and privacy of individuals, in particular shielded persons, that may result through unauthorised access, recording or disclosure of protected information by entrusted persons.

326. An example of when a person's conduct is authorised by a law of the Commonwealth or of a state or territory would be when an entrusted person is acting in accordance with one of the authorisations set out in clauses 31, 32, 33, 34, or 35. This might involve disclosing information in the course of performing their functions or duties for the purposes of the Bill (as authorised by clause 31) or to prevent a threat to life or health (as authorised by clause 32).

327. An example of when a person's conduct is in compliance with a requirement under a law of the Commonwealth or of a state or territory would be where a person is disclosing information as required under a search warrant or a subpoena from a court.

328. Note 1 under subclause 30(3) clarifies that the defendant will bear an evidential burden in relation to this exception. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden', the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the exception is made out. If this is done, the prosecution must refute the exception beyond reasonable doubt (section 13.1).

329. Placing the evidential burden on the defendant in relation to the exceptions in subclause 30(3) is appropriate because the facts in relation to the offence-specific exception would be peculiarly within the knowledge of the defendant. In particular, it would be impracticable to require the prosecution to prove that the defendant had no authorisation for the disclosure under any law. For the prosecution to prove this, it would likely need to examine a very large array of Commonwealth, state or territory laws in order to establish that there was no authorising law in the particular circumstances to the requisite burden of proof. In contrast, the defendant could readily and cheaply adduce evidence that suggests a reasonable possibility that an exception is applicable, by identifying the specific law that they claim the alleged unlawful conduct was in fact permitted under, or authorised by.

330. Both the AFP and the CDPP consider the availability of any defences when considering whether to investigate and prosecute criminal offences. In relation to prosecution decisions, the Prosecution Policy of the Commonwealth specifically requires the CDPP to take into account any lines of defence which are plainly open to, or have been indicated by, the alleged offender in deciding whether there is a reasonable prospect of a conviction being secured.

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

331. Subclause 30(4) of the Bill defines the terms ***entrusted person*** and ***protected information***.

332. An ***entrusted person*** means:

- the Secretary of the Department
- APS employees (as defined in section 7 of the *Public Service Act 1999*) in the Department
- a person whose services are made available to the Department who is:
  - an employee of an Agency as defined in the *Public Service Act 1999*
  - or an officer or employee of a State or Territory
  - an officer or employee of a government authority (defined in clause 5 to mean an authority of the Commonwealth, state or territory but not a local government authority)
  - an officer or employee of the government of a foreign country or an authority of a foreign country,
  - or an officer or employee of a public international organisation as defined in section 70.1 of the Criminal Code (for example multilateral international organisations such as the World Bank, World Trade Organization and International Monetary Fund)
- a contractor engaged to provide services to the Department in connection with an approved identity verification facility (whether the contractor is engaged directly or as a subcontractor), or
- an officer or employee of such a contractor whose duties relate wholly or partly to an approved identity verification facility.

333. ***Protected information*** means any of the following:

- information obtained by an entrusted person from electronic communications to or from an approved identity verification facility, or from the NDLFRS (paragraph (a))
- information about the making, content or addressing of an electronic communication to or from an identity verification facility that was obtained by an entrusted person in their capacity as an entrusted person (subparagraph (b)(i))
- information about identification information relating to a particular individual held in, or generated using, the NDLFRS, that was obtained by an entrusted person in their capacity as an entrusted person (subparagraph (b)(ii)); and
- information obtained by an entrusted person in their capacity as an entrusted person that would enable access to the DVS hub, Face Matching Services hub or the NDLFRS (paragraph (c)).

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

334. This clause would provide that an entrusted person may make a record of, disclose, or access information if they are doing so for the purposes of this Bill, or in the course of performing their functions or duties or exercising a power related to an approved identity verification facility.

335. This clause is intended to permit entrusted persons to disclose or record protected information in accordance with their normal work duties without committing an offence under subclause 30(1) of the Bill. For example, this could include a departmental officer disclosing information under a request for a person's own information under the *Freedom of Information Act 1982* (FOI Act) or Australian Privacy Principle 12.

336. This clause would provide an exception to the offences provided for in clause 30. The defendant will bear an evidential burden in relation to this exception.

Clause 32—Disclosure to lessen or prevent threat to life or health

337. Subclause 32 (1) provides that an entrusted person may disclose protected information if they reasonably believe that it is necessary to prevent a serious or imminent threat to the health or life of a person. The disclosure must be made for the purpose of preventing or lessening that threat.

338. The reasonable belief requirement under paragraph 32(1)(a) should be interpreted with reference to common law interpretations of the term in other legislation. In general, a subjective belief that the circumstances exist should be formed, supported by objective evidence that the belief is reasonable.

339. A 'serious' threat is one that poses a significant danger to one or more individuals. The likelihood of a threat occurring as well as the consequences if the threat materialises are both relevant in determining whether a threat is serious. The requirement that the threat must be 'imminent' is included to ensure that this clause would only permit an entrusted person to make a record of or access protected information while the threat still exists and urgent action is required to lessen or prevent it.

340. Examples of circumstances where disclosure may be permitted under this clause would include where it is unreasonable or impracticable to obtain the consent of the individual whose health or safety is threatened to the disclosure, recording or access given the imminence of the threat.

341. Subclause 32(2) clarifies that an entrusted person may make a record of or access protected information for the purpose of disclosing the protected information under subclause 32(1).

342. Clause 32 of the Bill is also intended to be read in a manner consistent with the *Australian Privacy Principles Guidelines* available on the OAIC website (see Chapter B in particular).[7]

343. This clause would provide an exception to the offences provided for in clause 30. The defendant will bear an evidential burden in relation to this exception.

Clause 33—Disclosure to IGIS official

344. Subclause 33(1) provides that an entrusted person may disclose protected information to an IGIS official for the purpose of the IGIS official exercising a power, or performing a duty, as an IGIS official. As defined in clause 5, an IGIS official includes the Inspector- of Intelligence and Security, as well as a staff member of the Inspector-General referred to in subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*.

345. Clause 33 is intended to enable the Inspector-General to obtain information on the use of the identity verification services by ASIO and ASIS, to assist in carrying out the Inspector-General's oversight duties and functions in relation to those agencies as provided in the *Inspector-General of Intelligence and Security Act 1986*. This information may include records of transactions held in the Face Matching Services hub, which are records that will not contain facial images, biometric templates or any other identification information about an individual.

346. Subclause 33(2) of the Bill provides that an entrusted person may make a record of, or access, protected information for the purpose of disclosing the information under subclause 33(1).

347. This clause would provide an exception to the offences provided for in clause 30. The defendant will bear an evidential burden in relation to this exception.

Clause 34—Disclosure to Ombudsman official

348. Subclause 34(1) of the Bill provides that an entrusted person may disclose protected information to an Ombudsman official for the purpose of the Ombudsman official exercising a power, or performing a function or duty, as an Ombudsman official. As defined in clause 5, an Ombudsman official includes the Commonwealth Ombudsman, the Deputy Commonwealth and staff of the Commonwealth Ombudsman, as referred to in subsection 31(1) of the *Ombudsman Act 1976*.

---

[7] See https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts.

349. This clause is intended to enable the Commonwealth Ombudsman to perform its functions the Ombudsman Act, including investigating complaints, as well as other functions conferred on the Ombudsman by the Ombudsman Act or any other Commonwealth Act, or any regulations made under those Acts.

350. Subclause 34(2) of the Bill provides that an entrusted person may make a record of, or access protected information for the purpose of disclosing the information under subclause 34(1).

351. This clause would provide an exception to the offences provided for in clause 30. The defendant will bear an evidential burden in relation to this exception.

Clause 35— Disclosure etc. with consent

352. Subclause 35(1) of the Bill provides that an entrusted person may make a record of, disclose or access protected information if they have the consent of the person to whom it relates. The recording, disclosing or access must be done in accordance with that consent.

353. Subclause 35(2) of the Bill provides that an entrusted person may make a record of, disclose, or access protected information that was held in, or generated using the NDLFRS (paragraph (a)) and was supplied by an authority of a State or Territory if that authority has consented to the recording, disclosure or access.

354. Currently, law enforcement occasionally request the Department to voluntarily disclose data held in or generated using the NDLFRS to support investigations. In order to disclose this data, the Department would seek the consent of the relevant jurisdiction that has responsibility for the data supplied to the NDLFRS. Subclause 35(2) of the Bill would enable disclosures of identification information by the Department under this circumstance.

355. A note to subclause 35(2) clarifies that the NDLFRS hosting agreement contains privacy requirements that relate to the authority as set out in subsection 13(2).

356. The concept of 'consent' in the Bill is intended to include express consent or implied consent. The discussion of the meaning of 'consent' in the *Australian Privacy Principles Guidelines* published on the OAIC website is also relevant to interpreting the meaning of 'consent' in the Bill.

Part 5—Miscellaneous

Clause 36—Simplified outline of this Part

357. Clause 36 contains a simplified outline of Part 5 of the Bill.

358. The simplified outline is included to assist readers to understand the substantive provisions of the Bill. The outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of the Bill.

Clause 37—No requirement for individuals to identify themselves

359. This clause outlines that the Act to be established by the Bill does not affect whether individuals have the option of not identifying themselves, or of using pseudonyms, when dealing with another person or body. The purpose of this clause is to clarify the scope of the Bill, which is to authorise the Department to establish, operate and maintain the identity verification services.

360. A note to subclause 37(1) clarifies that the Act to be established by the Bill does not affect the operation of Australian Privacy Principle 2, which provides that individuals must have the option of dealing anonymously or by pseudonym.

361. Subclause 37(2) of the Bill provides that subclause 37(1) does not affect the circumstances in which an identity verification service may be requested or provided.

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

362. Clause 38 permits the Secretary to, in writing, delegate the Secretary's powers under the Bill. The Secretary may only delegate powers and functions to an SES or acting SES employee in the Department.

363. This clause facilitates the practical implementation of the Bill. It is appropriate for the Secretary to be able to delegate his or her powers or functions to SES employees or acting SES employees within the Department to ensure the identity verification services can be efficiently administered. It is not practical, feasible or necessary for the Secretary to personally exercise the powers and functions of the scheme. This would lead to long delays and would not support prompt decision-making in relation to the development, operation and maintenance of the identity verification services.

364. The delegation power only allows delegation to SES employees or acting SES employees. This ensures that the powers and functions under the Bill are only exercisable by senior officers with experience and judgement in matters of public administration.

365. Note 1 to subclause 38(1) of the Bill clarifies that section 2B of the Acts Interpretation Act defines a SES employee and an acting SES employee. Section 2B of the Acts Interpretation Act defines both terms by reference to the Public Service Act. Section 34 of the Public Service Act defines SES employees to mean APS employees who are classified as SES employees under the Classification Rules. An acting SES employee is defined at section 7 of the Public Service Act as a non- SES employee who is acting in a position usually occupied by an SES employee.

366. Note 2 to subclause 38(1) of the Bill clarifies that section 34AA to 34A of the Acts Interpretation Act contains provision relating to delegation. Section 34AA provides that where an Act confers a power to delegate a function, duty or power, then the power of delegation shall not be construed as being limited to delegating the function, duty or power to a specified person. Rather it should be construed as including a power to delegate the function, duty or power to any person from time to time holding, occupying, or performing the duties of, a specified office or position, even if the office or position does not come into existence until after the delegation is given. As such, the delegation under clause 38 could be made to a position number, and SES employees who occupy that position number will have authority to exercise the delegated powers and functions.

367. Section 34AB of the Acts Interpretation Act provides that:

- delegations may be made generally or otherwise
- the powers that may be delegated do not include a power to delegate
- a function, duty or power that is exercised by a delegate is deemed to have been performed or exercise by the authority, and
- a delegation does not prevent the performance or exercise of a function, duty or power by the authority.

368. Section 34A of the Acts Interpretation Act provides that the Secretary would not be prevented from performing the function of exercising the power where a delegation is in place. The powers and functions can operate concurrently.

369. Subclause 38(2) of the Bill requires a delegate to comply with any written directions of the Secretary when performing their delegated powers or functions. This ensures that delegates are to administer the scheme consistent with the Secretary's views, if expressed in a written direction.

Clause 39—Publication of agreements and policies

370. Clause 39 supports public accountability and transparency by requiring that key documents associated with the identity verification services are publicly accessible on the Department's website.

371. Subclause 39(1) requires the Secretary to publish a copy of the following documents (and any document varying, terminating or revoking any of these documents) on the Department's website:

- the intergovernmental agreement
- a participation agreement
- the NDLFRS hosting agreement

- an instrument that causes a person or body to become, or to stop being, a party to a participation agreement or the NDLFRS hosting agreement, and
- a document that is approved by the Coordination Group provided for by the intergovernmental agreement and sets out an access policy for a service.

372. Subclause 39(2) of the Bill allows for the redaction of a part of the copy of any of the abovementioned documents prior to publication on the Department's website if the Secretary considers that publication of that part:

- creates a risk to the security of identification information or an approved identity verification facility
- unreasonably discloses personal information about an individual, or
- creates a risk to Australia's national security, within the meaning of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (if the document is a participation agreement, or a document that is approved by the Coordination Group provided for by the intergovernmental agreement and sets out an access policy for a service).

373. Section 8 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* defines national security to mean Australia's defence, security, international relations or law enforcement interests.

- Section 9 further defines the term ***security*** to have the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.
- Section 10 further defines the term ***international relations*** to mean political, military and economic relations with foreign governments and international organisations.
- Section 11 further defines ***law enforcement interests*** to include interests in:
    - avoiding disruption to national and international efforts relating to law enforcement, criminal intelligence, criminal investigation, foreign intelligence and security intelligence
    - protecting the technologies and methods used to collect, analyse, secure or otherwise deal with, criminal intelligence, foreign intelligence or security intelligence
    - the protection and safety of informants and of persons associated with informants
    - ensuring that intelligence and law enforcement agencies are not discouraged from giving information to a nation's government and government agencies.

374. Subclause 39(3) provides that, if the Secretary publishes a copy of a document that has been redacted in accordance with subclause 39(2) of the Bill, the Secretary must publish on the Department's website written reasons for not publishing the redacted part, except so far as the publication of the reasons would create a risk described in that subclause or unreasonably disclose personal information.

375. Subclauses 39(2) and (3) ensure that any sensitive information, the disclosure of which may cause a risk to the security of the development, operation and maintenance of the identity verification services, may be withheld by the Secretary when publishing the agreements, policies and other documents mentioned in subclause 39(1). For example, details of the cyber security arrangements for the identity verification facilities will be able to be removed from a participation agreement or the NDLFRS hosting agreement prior to publication on the Department's website. Further, personal information, for example, about a person in the Department or in an entity that has signed a participation agreement, may also be removed prior to publication of documents on the website.

376. These clauses strike an appropriate balance by enabling key information about the development, operation and maintenance of the identity verification services to be made publicly

available while appropriately protecting privacy and without creating a risk of harm to the security or of identification information and facilities, individuals, or Australia's national security.

Clause 40—Annual assessment by Information Commissioner

377. This clause provides that the Information Commissioner has the function of assessing and reporting on the operation and management of the approved identity verification facilities.

378. Subclause 40(1) of the Bill provides that the Information Commissioner has the function of assessing the operation and management of approved identity verification facilities and providing the Secretary with a written report on that assessment. The Information Commissioner would be required to perform both aspects of this assurance function within 6 months of the end of each financial year ending after the commencement of this subclause.

379. Examples of the matters which the Information Commissioner could consider in the annual assessment include whether the data generated by the approved identity verification facilities is the minimum necessary to effectively manage the hub, whether any complaints from the public have been received and what the responses to the complaints were and if any security breaches have occurred and what action was taken in response to any such breaches.

380. To facilitate the Information Commissioner's annual assurance function, the Secretary must ensure there is an appropriate arrangement in place with the Information Commissioner for providing information that they will need to conduct their assessments. Such an arrangement may be in place either before, on, or after the commencement of this clause. This is to ensure that any arrangements in place between the Department and the OAIC prior to commencement may continue upon the commencement of the Bill. The OAIC publishes such arrangements on its website.

Clause 41—Annual reporting

381. This clause outlines annual reporting requirements in relation to the identity verification services.

382. Subclause 41(1) of the Bill requires the Secretary to give the Minister a report for each financial year ending after the commencement of this clause, which will be the day after the Act receives the Royal Assent.

383. The annual report must include the following information:

- statistics relating to all requests in the financial year by or on behalf of government authorities, for a 1:1 matching services, which are the DVS and the FVS. This information is to be broken down by:
    - requesting authority (identified by name)
    - service requested
    - 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
    - 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
- statistics relating to all requests in the financial year from non-government entities for 1:1 matching service, which are the DVS and the FVS, including:
    - the total number of requests
    - the names of the non-government entities that made those requests
    - the number of those requests the response to which was that the requested comparison resulted in a match for an individual, and

    - the number of those requests the response to which was that the requested comparison did not result in a match for an individual
- the number of times 1:many matching services, which is the FIS, were used during the year and whether those requests were endorsed as required by clause 17 or not
- information about the accuracy of the systems for biometric comparison of facial images that are operated by the Department, which will be the NDLFRS, or the Department administering the Australian Passports Act, for the purposes of providing identity verification services
- the number of disclosures made to lessen or prevent a threat to life or health under subclause 32(1) in the financial year, and the number of individuals whose identification information was disclosed
- information about security incidents occurring in the financial year in connection with one or more of the approved identity verification facilities;
- 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;
- information about data breaches during the financial year there were connected with the operation of approved identity verification facilities and actions taken in the financial year in response to those breaches
- information about any party to a participation agreement or the NDLFRS hosting agreement, that had their ability to request an identity verification service terminated or suspended in the financial year due to non-compliance with either agreement or the access policy for the service
- any other information that relates to the financial year and either an identity verification service or the administration of this Act, and is required by the Minister.

384. Subclause 41(2) of the Bill provides that the annual report must not unreasonably disclose personal information about an individual. This is in addition to Department's privacy obligations concerning use and disclosure of personal information under Australian Privacy Principle 6.

385. Subclause 41(3) of the Bill would provide that the Secretary must give the Minister the annual report as soon as practicable after the end of the financial year and in any case within 6 months of the end of the financial year. For example, a report being prepared in July 2024 would relate to the 2023-24 financial year (being 1 July 2023 through to 30 June 2024) and would need to be provided to the Minister by 31 December 2024.

386. Subclause 41(4) of the Bill would provide that the Minister must table a copy of the annual report in each House of Parliament within 15 sitting days of that house after the Minister receives the report.

387. Subclause 41(5) of the Bill provides that, 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). This would ensure that the Minister has oversight over the use of services through the annual report, but that operationally sensitive information is removed before the report is tabled in Parliament and made public. This aligns with other approaches in Commonwealth legislation, including annual reporting requirements under the *Australian Security Intelligence Organisation Act 1979* (Cth) – see section 94(4)-(5).

388. Nothing in clause 41 of the Bill is intended to limit the Department's discretion to include any additional information in the annual report.

Clause 42—Fees

389. This clause would provide that the rules made by the Minister (as provided for under clause 44 of the Bill) may make provision in relation to the imposition, collection and recovery of fees.

390. Subclause 42(1) would provide that the rules may impose a fee for requests for identity verification services or in connection to the making of electronic communications to and from identity verification facilities.

391. This is intended to apply to the existing fee for service arrangement on which non-government organisations use the DVS, which is expected to provide the basis for those organisations to use the FVS. It is also intended to apply to any fee for service arrangements for use of the identity verification services by government agencies, if those were to be imposed. The rules will not be able to provide for the charging of fees directly to individuals who are having their identity verified through the use of the identity verification services.

392. Subclause 42(2) of the Bill would require that a fee prescribed by the Minister in rules must not be such as to amount to taxation. This clarifies that any prescribed fees are a fee for service and not a tax, which would engage section 53 of the Constitution.

Clause 43—Review of operations of this Act and provision of identity verification services

393. Subclause 43(1) of the Bill would provide that the Minister must cause a review of the operation of the Act and the provision of identity verification services to be started within two years of the commencement of clause 43.

394. A formal review will provide an opportunity to ensure that, among other things, the Act is operating as intended and that the privacy and security safeguards remain appropriate. A two-year period is appropriate for the review to be commenced as it allows sufficient time for participation agreements to be established for the DVS and the identity verification services to operate for a meaningful period of time before the review is undertaken.

395. Subclause 43(2) requires the Minister to cause a report of the review to be prepared and given to the Minister. The Minister must then table that report in each House of the Parliament within 15 sitting days after receipt of the report (subclause 43(3)).

Clause 44—Rules

396. Subclause 44(1) of the Bill provides that the Minister may make rules prescribing matters

- required or permitted by the Bill to be prescribed in the rules, or
- necessary or convenient to be prescribed for carrying out or giving effect to the Bill.

397. Any rules established under this section are legislative instruments for the purposes of the Legislation Act.

398. This is a broad rule-making power and will ensure that there is requisite authority to make such rules as are necessary to ensure the effective operation of the Act to be established by the Bill. The subclause is drafted in a manner to provide flexibility in prescribing matters by rules which may not have been foreshadowed at the time of establishment of the Act.

399. Subclause 44(2) of the Bill will provide clarification about things that the rules may not do, for the avoidance of doubt. It makes clear that any rules the Minister makes cannot:

- create an offence or civil penalty
- provide powers of arrest, detention, entry, search or seizure
- impose a tax
- set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in this Act, or

- directly amend the text of the Act to be established by the Bill.

400. The restrictions in subclause 44(2) mean that any of the above matters must be achieved by way of amendments to the Act.

401. Subclause 44(3) of the Bill provides that any rules made under subclause 44(1) will be subject to disallowance by Parliament. Subsection 44(1) of the Legislation Act provides that legislative instruments are not subject to disallowance if the enabling legislation facilitates the establishment or operation of an intergovernmental body or scheme involving one or more states and the instrument is made for the purposes of that body or scheme.

402. The effect of subclause 44(3) of the Bill is that, even though this Bill may fall within the types of enabling legislation referred to in subsection 44(1) of the Legislation Act, rules made under this Bill will be subject to parliamentary oversight and scrutiny through the disallowance process.

403. Subclause 44(4) of the Bill would make any rules prescribed under the Bill subject to sunsetting after ten years. Subsection 54(1) of the Legislation Act provides that legislative instruments are not subject to sunsetting if the enabling legislation facilitates the establishment or operation of an intergovernmental body or scheme involving one or more states and the instrument is made for the purposes of that body or scheme.

404. The effect of subclause 44(4) of the Bill is to provide that, even though this Bill may fall within the types of enabling legislation referred to in subsection 54(1) of the Legislation Act, rules made under this Bill will be subject to sunsetting. Sunsetting is an important scrutiny and transparency measure that will ensure that any rules made for the purpose of the Bill will be reviewed for currency and ongoing need.

IDENTITY VERIFICATION SERVICES (CONSEQUENTIAL AMENDMENTS) BILL 2023

Item 1—Name

1. This clause provides for the short title of the Act to be enacted by the Bill to be the *Identity Verification Services (Consequential Amendments) Act 2023*.

Item 2—Commencement

2. This clause provides for the commencement of each provision in the Consequential Amendments Bill) as set out in the table. Item 1 of the table provides that the whole of the Bill will commence on the day that is the later of:

(a) the start of the day after the Bill receives Royal Assent; or

(b) the commencement of the *Identity Verification Services Act 2023*.

3. However, as noted in Item 1, the provisions in the Consequential Amendments Bill do not commence if the proposed *Identity Verification Services Act 2023* does not commence. This reflects that the proposed amendments in the Consequential Amendments Bill is intended to support the operation of the identity verification services provided for in the Bill.

Item 3—Schedules

4. Clause 3 provides for the amendments outlined in the Schedule to the Consequential Amendments Bill to take effect according to their terms.

Schedule 1—Amendments

Australian Passports Act 2005 amendments

Item 1

5. Item 1 inserts the following definitions from the IVS Bill into subsection 6(1) of the Australian Passports Act:

- ***Document Verification Service*** has the same meaning as ***DVS*** which is defined at clause 15 of the IVS Bill. The DVS is a 1:1 matching identity verification service that performs biographic verification (such as verifying a date of birth) of identification information contained in an identity credential (state or territory issued licence, passport etc) against a particular government record.
- ***Face Verification Service*** has the same meaning as ***FVS*** is defined at clause 19 of the IVS Bill. The FVS is a 1:1 matching identity verification service that is used to verify biometric information (in this case a photograph of an individual) against a particular government record.

6. These definitions have been included to support new paragraph 46(da) (to be inserted by Item 3) and new section 46A (to be inserted by Item 6) which enable the disclosure of personal information for the purposes of the identity verification services.

Items 2 to 5

7. Item 2 and 3 amends section 46 of the Australian Passports Act and inserts new paragraph 46(1)(da) to allow the Minister to disclose personal information for the purpose of participating in one of the following services to share or match information relating to the identity of a person:

- the Document Verification Service or the Face Verification Service (new paragraphs 46(da)(i) to (ii)), or

- any other service, specified or of a kind specified in the Minister's determination (new paragraph 46(da)(iii)).

8. The Document Verification Service and Face Verification Service are used to securely verify the identity of Australians when providing access to critical services and functions, and by certain government agencies in order to protect the true identity of shielded persons (as defined in clause 5 of the Bill) and their associates.

9. To continue operating effectively, identity verification services depend on the ability to verify or match the biometric or biographic information on a person's identity credential against Commonwealth, State and Territory government records. An Australian Passport is one such identity credential that is relied upon by government and industry to verify their customer's identity through the identity verification service, and is the only government issued identity credential that enables biometric verification. Biometric verification is a highly secure way of verifying identity and is currently required to create a 'strong' MyGovID which is needed to access certain Centrelink and Australian Tax Office services.

10. New paragraph 46(1)(da) provides a clear legal basis for the disclosure of personal information for the purposes of participating in the identity verification services to share or match information relating to the identity of a person.

11. New paragraph 46(da)(iii) is intended to provide flexibility for the Minister to specify new services or kinds of services that may be used to share or match information relating the identity of a person in a determination. This ensures that a new type of identity verification service could be included should there be a need to do so. As technology advances, new services may be required to support the secure and efficient matching or verification of identity. Consistent with section 57 of the Australian Passports Act, such a determination will be a legislative instrument.

12. As reflected in the note at the end of the current section 46 of the Australian Passports Act, information disclosed under new paragraph 46(1)(da) must be dealt with in accordance with the Australian Privacy Principles.

13. Item 3 inserts new subsection 46(2) into the Australian Passports Act to clarify that specified personal information may be provided to the service before being disclosed to the person participating in the service. Section 46 currently provides for the Minister to make a determination to disclose specified information to a specified person. New subsection 46(2) ensures that disclosures under new paragraph 46(1)(da) aligns with the current technical operation of the identity verifications services and puts beyond doubt that specified personal information can be disclosed to the specified person via the services.

14. Item 5 specifies that the amendments to section 46 apply in relation to any information disclosed after the commencement of this item regardless of whether the information was obtained before or after that commencement.

Items 6 and 7

15. Item 6 inserts new section 46A into the Australian Passports Act to provide that the Minister may arrange for the use, under the Minister's control, of computer programs in disclosing personal information under new paragraph 46(1)(da) to a person participating in the Document Verification Service or the Face Verification Service.

16. New section 46A clarifies and enables automated disclosures of specified information via the Document Verification Service or Face Verification Service. This addresses the fact that current section 46 of the Australian Passports Act does not clearly contemplate disclosures being made through an entirely automated decision-making process.

17. Importantly, new section 46A only permits automated disclosures in relation to the 1:1 matching services, defined in clause 5 to mean the Document Verification Service or Face Verification Service. It does not allow for automated disclosures for any other purposes under the Australian Passports Act, including in relation to the Face Identification Service. This aligns with the

current operational needs of the Department of Foreign Affairs and Trade and ensures that, in all other circumstance, the appropriateness, necessity and legal authority to support disclosures of personal information is considered by a decision-maker in DFAT or the Minister.

18. New section 46A complements new paragraph 46(1)(da) and subsection 46(2). New section 46A allows for the Minister to use an appropriately controlled computer program to make decisions of personal information. The disclosure is authorised by new paragraph 46(1)(da) and the fact that the personal information may be dealt with by a system before it is disclosed to the person is confirmed by new subsection 46(2). In combination, this comprehensively authorises the operation of the Document Verification Service and Face Verification Service in relation to Australian travel documents regulated by the Australian Passports Act.

19. New section 46A reflects the technical operation of the identity verification service, which will operate on an automated query and response basis. Requests will need to be received and responded to in a timeframe that precludes the exercise of human discretion in deciding whether to disclose the information in each case. The current scale of the Document Verification Service and the future uses of the Face Verification Service will make human intervention infeasible.

20. Item 7 clarifies that section 46A applies in relation to any disclosures of personal information occurring after the commencement of this item, regardless of whether the information was obtained before or after that commencement