IDENTITY VERIFICATION SERVICES RULES 2024

EXPLANATORY STATEMENT

Issued by authority of the Attorney-General

under section 44 of the *Identity Verification Services Act 2023*

PURPOSE AND OPERATION OF THE INSTRUMENT

Subsection 44(1) of the *Identity Verification Services Act 2023* (the Act) provides that the Minister may, by legislative instrument, make rules prescribing matters required or permitted by the Act to be prescribed by the rules, or necessary or convenient to be prescribed for carrying out or giving effect to the Act.

The purpose of the Identity Verification Services Rules 2024 (the Rules) is to prescribe the following matters, which are needed to support the operation of the identity verification services and are required or permitted to be made under the Act:

- listing state and territory privacy laws and government authorities, which must be listed for the purposes of *participation agreements* (at Part 2)
- listing state and territory privacy laws, which must be listed for the purpose of the *NDLFRS hosting agreement* (at Part 3)
- setting fees that government authorities and non-government entities must pay to connect to, and request the use of, the identity verification services (at Part 4).

The 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.

The Act provides a legislative framework to support the secure and efficient operation of the identity verification services, subject to strong privacy safeguards and oversight arrangements. Specifically, the Act establishes a framework that authorises:

- government and industry to make requests for 1:1 matching services for the purpose of verifying identity through the Document Verification Service (DVS) and the Face Verification Service (FVS)
- the National Driver Licence Facial Recognition Solution (NDLFRS), which facilitates 1:1 matching of identity through driver licences

- limited government agencies to make requests for a 1:many matching service through the Face Identification Service (FIS) for the purpose of protecting the identity of persons with a legally assumed identity
- the responsible Commonwealth department – in this case the Attorney-General's Department (the department) – to develop, operate and maintain the 3 approved identity verification facilities needed to support the operation of the identity verification services.

The operation of the identity verification services is subject to strong privacy safeguards, security measures and oversight measures outlined in the Act. This ensures that the community can benefit from secure and fast identity verification, without compromising their personal information. It will also support more Australians to establish a digital ID in order to access critical services, and will support broader efforts to reduce identity crime.

The Rules are consistent with subsection 44(2) of the Act which places important limitations on the scope of the rule-making power to ensure 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.

As provided by subsection 44(1) of the Act, the Rules would be a legislative instrument for the purposes of the *Legislation Act 2003* (Cth) (Legislation Act).

Subsection 44(3) of the Act means that the Rules will be subject to parliamentary oversight and scrutiny through the disallowance process provided in the Legislation Act.

Subsection 44(4) of the Act clarifies that the Rules will also be subject to sunsetting after 10 years. Sunsetting is an important scrutiny and transparency measure that will ensure the Rules are reviewed for currency and ongoing need.

Details of the Rules are set out in **Attachment A**.

CONSULTATION

Before making the Rules, and as required by subsection 44(1B) of the Act, the Attorney-General published a draft of the Rules on the department's website and invited public submissions. The draft Rules were published for a 28-day period, as required under subparagraph 44(1B)(a)(ii) of the Act.

There were 8 submissions made during the consultation period between 3 April 2024 and 1 May 2024, all of which were considered and, where appropriate, changes were made to the finalised Rules.

Targeted consultation was undertaken on the draft Rules with relevant industry organisations and Commonwealth, states and territories government authorities, including:

- Commonwealth data holding agencies, and relevant state and territory government agencies
- Commonwealth law enforcement, intelligence and integrity agencies
- key industry stakeholders, in particular, Gateway Service Providers.

In accordance with paragraph 44(1B)(b) of the Act, the Attorney-General also consulted the Information Commissioner on the Rules as they relate to the privacy functions (within the meaning of the *Australian Information Commissioner Act 2010*).

REGULATION IMPACT STATEMENT

The Office of Impact Analysis advised that an Impact Analysis is not required as the Rules are unlikely to have a more than minor impact (OIA23-06305).

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

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

The Identity Verification Services Rules 2024 (the Rules) are 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 legislative instrument

Subsection 44(1) of the *Identity Verification Services Act 2023* (the Act) provides that the Minister may, by legislative instrument, make rules prescribing matters required or permitted by the Act to be prescribed by the rules, or necessary or convenient to be prescribed for carrying out or giving effect to the Act.

The purpose of the Identity Verification Services Rules 2024 (the Rules) is to prescribe the following matters, which are needed to support the operation of the identity verification services and are required or permitted to be made under the Act:

- listing state and territory privacy laws and government authorities, which must be listed for the purposes of *participation agreements* (at Part 2)
- listing state and territory privacy laws, which must be listed for the purpose of the *NDLFRS hosting agreement* (at Part 3)
- setting fees that government authorities and non-government entities must pay to connect to, and request the use of, the identity verification services (at Part 4).

The Rules reflect the outcome of consultations with the public and the Australian Information Commissioner, as required under the Act. To facilitate these consultations, the department also engaged with key stakeholders, including state and territory government agencies and the largest industry users of the services – Gateway Service Providers.

The Rules are also consistent with section 44(2) of the Act which places important limitations on the scope of the rule-making power to ensure 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.

The 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.

The Act provides a legislative framework to support the secure and efficient operation of the identity verification services, subject to strong privacy safeguards and oversight arrangements. Specifically, the Act establishes a framework that authorises:

- government and industry to make requests for 1:1 matching services for the purpose of verifying identity through the Document Verification Service (DVS) and the Face Verification Service (FVS)
- the National Driver Licence Facial Recognition Solution (NDLFRS), which facilitates 1:1 matching of identity through driver licences
- limited government agencies to make requests for a 1:many matching service through the Face Identification Service (FIS) for the purpose of protecting the identity of persons with a legally assumed identity
- the responsible Commonwealth department – in this case the Attorney-General's Department (the department) – to develop, operate and maintain the 3 approved identity verification facilities (approved facilities) needed to support the operation of the identity verification services.

The operation of the identity verification services is subject to strong privacy safeguards, security measures and oversight measures outlined in the Act. This ensures that the community can benefit from secure and fast identity verification, without compromising their personal information. It will also support more Australians to establish a digital ID in order to access critical services, and will support broader efforts to reduce identity crime.

The Rules would commence on 14 June 2024. In accordance with section 2 of the Act, the remaining provisions in the Act will commence on the same date, giving full effect to the entirety of the Act.

Human rights implications

The measures in Part 2 and 3 of the Rules engages the *prohibition on interference with privacy, and right to reputation*, under article 17 of the International Covenant on Civil and Political Rights (ICCPR).

The prohibition on interference with privacy contained in article 17 of the ICCPR

Article 17 of the ICCPR prohibits unlawful or arbitrary interference with a person's privacy, family, home and correspondence, and prohibits unlawful attacks on a person's reputation. The United Nations Human Rights Committee has interpreted the right to privacy as comprising freedom from unwarranted and unreasonable intrusions into activities that society recognises as falling within the sphere of individual autonomy.

The right to privacy may be limited where the limitation is lawful and not arbitrary. The use of the term 'arbitrary' means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances.
The United Nations Human Rights Committee has interpreted 'reasonableness' to imply that any limitation must be proportionate and necessary to achieve a legitimate objective.

The following measures in the Rules would engage the right to privacy:

- prescribing state and territory privacy laws and government authorities for the purposes of *participation agreements* (at Part 2)
- prescribing state and territory privacy laws for the purpose of the *NDLFRS hosting agreement* (at Part 3).

Participation agreements

The Act includes important safeguards and protections to ensure that access to, and operation of, the identity verification services does not compromise the privacy of Australians and the security of information. A number of these privacy safeguards and protections are set out in participation agreements, which are agreements between relevant entities and the Attorney-General's Department (the department), representing the Commonwealth. All entities seeking to make a request for identity verification services must be a party to a participation agreement and meet the privacy obligations and requirements set out in the Act.

To be a party to a participation agreement, entities must satisfy one of the requirements set out in subsection 9(1) of the Act. Of relevance to Part 2 of the Rules, these require the entity to:

- be subject to a privacy law of a state or territory prescribed in the rules (subparagraph 9(1)(b)(ii) of the Act)
- be a government authority prescribed in the rules (paragraph 9(1)(d) of the Act).

Section 5 of the Rules prescribes state and territory privacy laws for the purposes of subparagraph 9(1)(b)(ii) of the Act. By prescribing these laws, the Rules promote the right to privacy by ensuring relevant entities, in particular state and territory government agencies, are subject to an

appropriate privacy law in order to become a party to a participation agreement and engage with the identity verification services.

The Rules do not list laws from South Australia or Western Australia, as these jurisdictions do not currently have privacy laws in force. Government agencies in these jurisdictions will need to satisfy another requirement at subsection 9(1) of the Act in order to become a party to a participation agreement, including agreeing to comply with the Australian Privacy Principles. This means government agencies in these jurisdictions that are party to a participation agreement will have obligations with respect to the collection, use and disclosure of personal information.

Furthermore, South Australian and Western Australian government agencies that become parties to a participation agreement, as well as other parties to the agreement, will be subject to the privacy safeguards in the Act which seek to protect the personal information of Australians when engaging with the identity verification services. These safeguards and protections include: privacy impact assessments; requirements to report security breaches and data breaches; complaint handling mechanisms; annual compliance reporting and transparency about how information will be collected, used and disclosed. Non-compliance with these privacy safeguards may lead to the suspension or termination of access to the services.

Section 6 of the Rules prescribes Commonwealth intelligence and integrity agencies for the purposes of paragraph 9(1)(d) of the Act. Section 6 may limit the right to privacy provided in Article 17 of the ICCPR, as it enables the prescribed agencies to become a party to a participation agreement despite not being subject to a privacy law or the Australian Privacy Principles.

While the right to privacy may be limited by section 6, the purpose of this limitation is for the legitimate objective of ensuring that the prescribed agencies are able to access the services for critical operational purposes. For example, certain agencies prescribed at section 6 may seek to use the FIS for the purpose of protecting the identity of shielded persons and their associates.

Shielded persons are defined in section 5 of the Act 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). This capability ensures agencies can protect the safety of undercover officers, and prevent active investigations from being compromised.

If they were not prescribed in the Rules, the Commonwealth agencies listed at section 6 would be unable to enter into a participation agreement unless they agreed to voluntarily opt-in to the *Privacy Act 1988* (Cth) (Privacy Act) or the Australian Privacy Principles, which could have disproportionate operational implications and other undesirable outcomes.

Despite being exempt from the Privacy Act, as parties to a participation agreement, these Commonwealth agencies will be subject to the privacy safeguards and obligations in the Act in relation to their use of the identity verification services. These safeguards and obligations govern how parties are authorised to collect, use and disclose identification information, and require such entities to implement certain procedures and take action to protect the information of individuals when engaging with the services.

For example, paragraph 9(2)(e) of the Act requires that parties to participation agreements notify the Department of any breaches of security relating to the identity verification services. This obligation, along with the requirement for the Department to report to the Information Commissioner (paragraph 9(2)(f)), is intended to align with, and be read in a manner consistent with, the Notifiable Data Breaches scheme under the Privacy Act.

The Commonwealth agencies prescribed at section 6 also have appropriate privacy rules and safeguards in place, and are subject to independent oversight and scrutiny. For example, the Inspector-General of Intelligence and Security oversee the Australian Criminal Intelligence Commission, Australian Security Intelligence Organisation, Australian Secret Intelligence Service and Office of National Intelligence; and the National Anti-Corruption Commission is overseen by the Parliamentary Joint Committee on the National Anti-Corruption Commission and an Inspector of the National Anti-Corruption Commission, and is subject to inspections by the Commonwealth Ombudsman.

For the reasons cited above, it is a reasonable, necessary and proportionate limitation on the right to privacy to prescribe the Commonwealth agencies at section 6 of the Rules.

NDLFRS hosting agreement

The NDLFRS is an electronic database of state and territory identity documents (such as driver licences), and systems and templates that enable identity verification to occur against facial images in the database. The Act sets out security measures and obligations to protect personal information stored on the NDLFRS. These measures are outlined at section 13 of the Act and reflected in the NDLFRS hosting agreement.

The NDLFRS hosting agreement 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. All states and territories that upload, or intend to upload, data to the NDLFRS are required to be a party to the NDLFRS hosting agreement.

Section 7 of the Rules prescribes state and territory privacy laws for the purpose of the NDLFRS hosting agreement. This promotes the right to privacy by ensuring that state and territory government authorities are subject to their jurisdiction's privacy law in order to become a party to the NDLFRS hosting agreement and contribute data to the database.

The Rules do not list laws from South Australia or Western Australia, as these jurisdictions do not currently have privacy laws in force. Government agencies in these jurisdictions will need to satisfy another requirement at subsection 13(2) of the Act in order to become a party to a participation agreement, including agreeing to comply with the Australian Privacy Principles. This means that all parties will have obligations with respect to the collection, use and disclosure of personal information.

Furthermore, South Australian and Western Australian government agencies that become parties to the NDLFRS hosting agreement, as well as other parties to the agreement, will be subject to the privacy safeguards and obligations in the Act. This includes requirements for state or territory authorities to: inform individuals if their information is stored in the NDLFRS (and provide for a mechanism by which those persons can correct any errors); inform the department and individuals whose information is stored in the NDLFRS of any data breaches; establish a complaints mechanism; and report annually to the department on the party's compliance with the agreement.

Non-compliance with these privacy safeguards may lead to the suspension or termination of the ability for the party to request the identity verification services involving the NDLFRS.

Conclusion

The Rules are compatible with human rights and freedoms recognised or declared in the international instruments listed in the definition of human rights in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*. To the extent that measures in the Rules limit those rights and freedoms, such limitations are reasonable, necessary and proportionate to a legitimate objective.

Attachment A

NOTES ON SECTIONS

PART 1 – Preliminary

This Part would deal with a number of preliminary matters, including the commencement of the Rules, the authority under which they would be made, and definitions.

Section 1 – Name

This section would provide that the name of the Rules is the *Identity Verification Services Rules 2024*.

Section 2 – Commencement

This section would provide that all provisions in the Rules commence on 14 June 2024. As the Rules are set to commence on the same date as 6 months after the Act received the Royal Assent, the entirety of the Act will also commence on 14 June 2024.

To ensure the Minister was empowered to make these rules, sections 1 to 14, 42 and 44 in the Act commenced the day after the Act received the Royal Assent. Section 2 of the Act provides that all remaining provisions in the Act (sections 15 – 41 and section 43) would commence the earlier of either:

- the commencement of rules made under the rule-making power at section 44 of the Act, or
- 6 months after the Act received the Royal Assent.

These remaining provisions relate to requesting and providing the identity verification services, and cover the obligations and requirements for governments and entities seeking to use and provide access to data for the purposes of the DVS, FVS and FIS.

This approach to commencement provided sufficient opportunity for the Attorney-General to undertake and consider the outcome of consultations on the Rules, as required under paragraph 44(1B) of the Act. It also provided certainty and clarity to industry during the public consultation period as to when their obligations under the Act and, in particular, when the fees at Part 4 of the Rules would take effect.

Section 3 – Authority

This section would provide that the Rules are made under the *Identity Verification Services Act 2023.*

Section 4 – Definitions

This section would define the following term used in the Rules:

- ***Act*** means the *Identity Verification Services Act 2023.*

PART 2 – Participation agreements

This Part would set out state and territory privacy laws and government authorities for the purposes of participation agreements.

The Act includes important safeguards and protections to ensure that access to, and operation of, the identity verification services does not compromise the privacy of Australians and the security of information. For entities seeking to make requests for the services, these privacy safeguards and protections are primarily outlined at sections 9 and 10 of the Act.

The privacy safeguards and protections in the Act will be set out in participation agreements, which are agreements between relevant entities and the Attorney-General's Department (the department), representing the Commonwealth.

Participation agreements are defined at section 8 of the Act. They support the administration and operation of the identity verification services, protect the security and privacy of identification information, and provide additional transparency and oversight arrangements regarding the use and operation of the services.

All entities seeking to make requests for the identity verification services will be required to be a party to a participation agreement. This requirement is set out in paragraph 15(1)(b) of the Act for the DVS, subsection 19(a) for the FVS and paragraph 17(1)(a) for the FIS.

To be a party to a participation agreement, entities must satisfy one of the requirements set out in subsection 9(1) of the Act. Of relevance to Part 2 of the Rules, these require the entity to:

- be subject to a privacy law of a state or territory prescribed in the rules (subparagraph 9(1)(b)(ii) of the Act), or
- be a government authority prescribed in the rules (paragraph 9(1)(d) of the Act).

Section 5 – Prescribed privacy laws

This section would prescribe the following list of state and territory privacy laws for the purpose of subparagraph 9(1)(b)(ii) of the Act:

(a) the *Privacy and Personal Information Protection Act 1998* (NSW);

(b) the *Privacy and Data Protection Act 2014* (Vic);

(c) the *Information Privacy Act 2009* (Qld);

(d) the *Personal Information Protection Act 2004* (Tas);

(e) the *Information Privacy Act 2014* (ACT);

(f) the *Information Act 2002* (NT).

By prescribing these state and territory privacy laws, section 5 of the Rules would ensure entities that are subject to these laws, including relevant state and territory government agencies, can satisfy paragraph 9(1)(b) for the purposes of becoming a party to a participation agreement.

The Rules do not list laws from South Australia or Western Australia, as these jurisdictions do not currently have privacy laws in force. Government agencies in these jurisdictions will need to satisfy another requirement at paragraph 9(1) of the Act in order to become a party to a participation agreement. This includes being subject to the *Privacy Act 1988* (Cth) (Privacy Act) or agreeing to comply with the Australian Privacy Principles.

Section 6 – Prescribed government authorities

Section 6 of the Rules would prescribe the following government authorities for the purpose of paragraph 9(1)(d) of the Act:

(a) the Australian Criminal Intelligence Commission;

(b) the Australian Secret Intelligence Service;

(c) the Australian Security Intelligence Organisation;

(d) the National Anti-Corruption Commission;

(e) the Office of National Intelligence.

Section 6 of the Rules would enable these Commonwealth agencies to satisfy paragraph 9(1)(d) of the Act for the purposes of becoming a party to a participation agreement. Paragraph 9(1)(d) of the Act is intended to apply to those agencies that need to use the services but cannot comply with another requirement at subsection 9(1).

These Commonwealth integrity and intelligence agencies have a demonstrated operational need to use the identity verification services. For example, certain agencies prescribed at section 6 may seek to use the FIS for the purpose of protecting the identity of shielded persons and their associates. Shielded persons are defined in section 5 of the Act 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). This capability ensures agencies can protect the safety of undercover officers, and prevent active investigations from being compromised.

The Commonwealth agencies prescribed at section 6 of the Rules cannot satisfy another requirement in subsection 9(1) of the Act because they are exempt from complying with the Privacy Act and the

Australian Privacy Principles. Unless prescribed under section 6, these agencies would be unable to enter into a participation agreement unless they agreed to voluntarily opt-in to the Privacy Act or the Australian Privacy Principles, which could have disproportionate operational implications and other undesirable outcomes.

Despite being exempt from the Privacy Act, these Commonwealth agencies will be subject to the privacy safeguards and obligations in the Act in relation to their use of the identity verification services. These safeguards and obligations govern how parties to participation agreements are authorised to collect, use and disclose identification information, and require such entities to implement certain procedures and take action to protect the information of individuals when engaging with the services.

For example, paragraph 9(2)(e) of the Act requires that parties to participation agreements notify the department of any breaches of security relating to the identity verification services. This obligation, along with the requirement for the department to report to the Information Commissioner (paragraph 9(2)(f)), is intended to align with, and be read in a manner consistent with, the Notifiable Data Breaches scheme under the Privacy Act.

The Commonwealth agencies prescribed at section 6 also have appropriate privacy rules and safeguards in place, and are subject to independent oversight and scrutiny. For example, the Inspector-General of Intelligence and Security oversee the Australian Criminal Intelligence Commission, Australian Security Intelligence Organisation, Australian Secret Intelligence Service and Office of National Intelligence; and the National Anti-Corruption Commission is overseen by the Parliamentary Joint Committee on the National Anti-Corruption Commission and an Inspector of the National Anti-Corruption Commission, and is subject to inspections by the Commonwealth Ombudsman.

Part 3 – NDLFRS hosting agreement

This Part would set out state and territory privacy laws for the purposes of the NDLFRS hosting agreement.

As provided at section 5 of the Act, the NDLFRS is a system that is developed, operated and maintained by the Department under Part 2 of the Act that consists of 2 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 the database

- a system for biometric comparison of facial images with facial images that are in that database.

The primary purpose of the NDLFRS is to create an electronic centralised repository of state and territory identity information (including the individual's given name/s, photo, and date of birth) and information associated with the identity credential (for example, whether a licence has been reported as lost or stolen). The NDLFRS enrols the supplied images 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.

The Act sets out security measures and obligations to protect personal information stored on the NDLFRS. These measures are outlined at section 13 of the Act and reflected in the NDLFRS hosting agreement.

The NDLFRS hosting agreement is defined at subsection 13(1) of the Act as 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.

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.

To be a party to the NDLFRS hosting agreement, state and territory government authorities must satisfy one of the requirements set out at subsection 13(2) of the Act. Of relevance to Part 3 of the Rules, paragraph 13(2)(a) of the Act requires a government authority that is a party to the agreement to be subject to a state or territory privacy law that is prescribed in rules.

Section 7 - Prescribed privacy laws

Section 7 of the Rules would prescribe the following list of state and territory privacy laws for the purpose of subparagraph 13(2)(a)(ii) of the Act:

(a) the *Privacy and Personal Information Protection Act 1998* (NSW)

(b) the *Privacy and Data Protection Act 2014* (Vic)

(c) the *Information Privacy Act 2009* (Qld)

(d) the *Personal Information Protection Act 2004* (Tas)

(e) the *Information Privacy Act 2014* (ACT)

(f) the *Information Act 2002* (NT).

By prescribing these state and territory privacy laws, section 7 of the Rules would enable state and territory government agencies subject to those laws to satisfy paragraph 13(2)(a) of the Act for the purposes of becoming a party to the NDLFRS hosting agreement.

South Australian and Western Australian laws are not included as these jurisdictions do not currently have privacy laws in force. Government agencies in these jurisdictions will need to satisfy another requirement at subsection 13(2) of the Act for the purpose of the NDLFRS hosting agreement. This includes being subject to the Privacy Act or agreeing to comply with the Australian Privacy Principles.

Part 4 - Fees

Part 4 of the draft Rules provide:

- fees for connecting to the approved identity verification facilities
- fees for requests for identity verification services.

The fees align with, and are authorised by, section 42 of the Act. Section 42 provides that rules made by the Minister (as provided for under section 44 of the Act) may make provisions in relation to the imposition, collection and recovery of fees, including fees for requests for identity verification services or in connection to the making of electronic communications to and from the approved identity verification facilities.

Subsection 42(2) of the Act requires 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.

Section 8 – Fees for connection to approved identity verification facility

The application of connection fees would vary depending on:

(1) whether the authority or entity seeking to connect to an approved identity verification facility is a government authority or non-government entity
(2) the approved identity verification facility the authority or entity is seeking to connect to
(3) whether the authority or entity is seeking a new connection to an approved identity verification facility, and the number of document types or kinds of documents an entity intends to use to make requests for the identity verification services
(4) whether the authority or entity has an existing connection and seeks to be connected in relation to one or more additional 'kinds of documents' (listed at subsection 8(5) of the Rules).

Examples are provided below to illustrate the application of connection fees in each of the above circumstances.

Subsection 8(1) of the Rules would provide that, for the purposes of paragraph 42(1)(a) of the Act, a fee is payable by a government authority or non-government entity for a connection to an approved identity verification facility mentioned in an item of the table in subsection 8(4) of the Rules.

A government authority is defined at section 5 of the Act as 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 Act. A non-government entity is defined at section 5 of the Act to mean a person or body, other than the Commonwealth, a state or territory or a government authority.

Approved identity verification facility is defined at section 5 of the Act to mean the DVS Hub, the Face Matching Service Hub and the NDLFRS, which are defined separately in the Act. The approved identity verification facilities provide the technical capability for a request to be made for an identity verification service, and supports the operation of the NDLFRS. They operate as a router to securely communicate requests from entities seeking to verify identity to the government agencies holding the data, and the outcome of those requests back to the requesting agencies. The facilities operate subject to safeguards, limitations and oversight arrangements outlined in the Act.

A note to subsection 8(1) clarifies that an authority or entity may have more than one connection to an approved identity verification facility. Business needs may necessitate an authority or entity to have multiple connections to the same facility, and for each of those connections to be related to different kinds of documents (listed at subsection 8(5) of the Rules). The application of fees in this scenario is discussed further in examples 4 and 5 below.

Subsection 8(2) of the Rules provides that, subject to subsection (3), the amount of the fee for the connection is the sum of:

(a) the amount mentioned in column 2 in the table at subsection 8(4) that covers the facility
(b) the amount worked out by multiplying:
    (i) the number of kinds of documents (see subsection (5)) for which the authority or entity is seeking to be able to request identity verification services using the facility, by
    (ii) the amount mentioned in column 3 in the tabled at subsection 8(4).

Column 2 in the table at subsection 8(4) are one-off ‘base connection amounts’ that are only payable when an authority or entity is seeking a new connection to an approved identity verification facility.

Column 3 is the additional amount that authorities or entities must pay for each kind of document (listed at subclause 8(5)) they seek to be connected to and be able to request identity verification services using the facility.

A note to subsection (2) clarifies that the provision applies in circumstances where an authority or entity:

(a) is not otherwise connected to the facility; or
(b) is seeking to increase its number of connections to the facility.

The application of fees in this scenario is discussed further at examples 1-5 below.

Example 1 – Non-government entity first time connection to the approved identity verification facility

A non-government entity seeks to connect to the Face Matching Service Hub. The organisation intends to make requests for the FVS using Australian passports and driver licences, which are 2 kinds of documents listed at subsection 8(5). This entity would pay the following one-off connection fee:

- Base connection amount: $31,139.45
- Additional cost per kind of document: $850 x 2 = $1,700

This means the entity would pay a total one-off connection fee of $32,839.45 (excl GST).

Example 2 – Commonwealth department connecting to an approved identity verification facility

A Commonwealth department is seeking to connect to the DVS Hub and intends to make requests for the DVS using driver licences and Medicare cards. The Commonwealth department would pay the following connection fees:

- Base connection amount: $5,470.95
- Additional cost per kind of document: $454.55 x 2 = $909.10

This means the Commonwealth department would pay a total one-off connection fee of $6,380.05 (excl GST). Other one-off costs associated with this connection would be met by Commonwealth funding.

Example 3 – Non-government entity connecting to both approved identity verification facilities

A non-government entity seeks to connect to the DVS Hub and intends to make requests for the DVS using Medicare cards, change of name certificates and birth certificates.

The entity also seeks to connect to the Face Matching Service Hub and intends to make requests for the FVS using Australian passports and driver licences.

This entity would pay the following connection fee:

For the DVS Hub

- Base connection amount: $24,610.40
- Additional cost per kind of document: $454.55 x 3 = $1,363.65
- Total for DVS Hub: $25,974.05

For the Face Matching Service Hub

- Base connection amount: $31,139.45
- Additional cost per kind of document: $850 x 2 = $1,700
- Total for Face Matching Service Hub: $32,839.45

In practice, this means the entity would pay a total one-off connection fee of $58,813.50 (excl GST).

Example 4 – Non-government entity second connection to the same approved identity verification facility (one existing connection)

A non-government entity is already connected to the Face Matching Service Hub in relation to Australian passports and driver licences.

For operational reasons, the entity determines it requires an additional connection to the Face Matching Service Hub in relation to 3 kinds of documents – Australian passports, driver's licences and visas.

While the entity already has one connection to the Face Matching Service Hub, because it is seeking a new connection the same facility, it would be subject to the following fees:

- Base connection amount: $31,139.45
- Additional cost per kind of document: $850 x 3 = $2,550

This means the entity would pay a total one-off connection fee of $33,689.45 (excl GST).

Example 5 – Commonwealth department 2 first-time connections to the same approved identity verification facility

A Commonwealth department is not connected to any approved identity verification facility. Due to its various functions and responsibilities, the department determines that it requires 2 'first time' connections to the DVS Hub.

One connection will require access to 3 kinds of documents – Australian passports, birth certificates, and visas. The other connection will require access to two kinds of documents – driver licences and visas.

The department's total connection fee is as follows:

Connection 1

- Base connection amount: $5,470.95
- Additional cost per kind of document: 3 x $454.55.

Connection 2

- Base connection amount: $5,470.95
- Additional cost per kind of document: 2 x $454.55.

This means the department would pay a total one-off connection fee of $13,214.65 (excl GST).

Subsection 8(3) of the Rules would clarify the application of the fees in circumstances where an authority or entity with an existing connection is seeking to ensure that existing connection can be used to make requests in relation to one or more new kinds of documents.

Subsection 8(3) would provide that, if:

(a) the authority or entity has an ***existing connection*** to the facility; and
(b) the authority or entity seeks to replace the existing connection with a connection to the facility that would enable the authority or entity to request identity verification services in relation to:
    (i) one or more kinds of documents (see subsection (5)) in relation to which the existing connection enables the authority or entity to request identity verification services; and
    (ii) one or more other kinds of documents;

the amount of the fee for the replacement connection is the amount worked out by multiplying:

(c) the number of kinds of documents in relation to which subparagraph (b)(ii) applies; by
(d) the amount mentioned in column 3 in the tabled at subsection 8(4) the relevant approved identity verification facility.

A note to subsection 8(3) would clarify that this provision would apply if the number of connections an authority or entity has to an identity verification facility will not change. This means that subsection 8(3) is not relevant in circumstances where an authority or entity is connecting to an approved identity verification facility for the first time, or seeking multiple connections to the same facility. Subsection 8(2) would be relevant in these scenarios.

To further clarify the application of subsection 8(3), the note provides the following example:

> A non-government entity has a connection to the DVS Hub, and can make requests using that facility for identity verification services in relation to the kinds of documents mentioned in paragraphs (5)(a), (b) and (c). The entity would like to replace that connection with a connection that enables them to request identity verification services in relation to the kinds of documents mentioned in paragraphs (5)(a), (b), (c), (d) and (e).
>
> Because there are 2 kinds of documents in relation to which subparagraph (b)(ii) of this subsection will apply (the kinds of documents mentioned in paragraphs (5)(d) and (5)(e)), the amount of the fee for the replacement connection will be $909.10 (see column 3 of item 1 of the table in subsection (4)).

A replacement connection does not replace the entirety of an authority or entity's existing connection to an approved identity verification facility. Instead, the act of 'replacing' an existing connection would enable an authority or entity to make requests in relation to one or more additional kinds of documents through the facility as well as the kinds of documents that relate to its existing connection. As such, the authority or entity is not required to pay an additional 'base connection amount' (column 2 in the table at subsection 8(4)).

In this circumstance, as provided by paragraph 8(3)(c) and (d), an authority or entity would only be subject to the fee in column 3 for each additional kind of document in relation to which the entity is seeking to be able to request identity verification services using the facility.

Example 6 below clarifies the application of the fees in this circumstance.

Example 6 – Non-government entity seeking to connect to additional documents

A non-government entity is already connected to the DVS Hub in relation to birth certificates and Australian passports. Due to a change in operations, the organisation seeks to connect to an additional 2 documents – driver's licences and Medicare cards. The entity would pay the following one-off fee:

- Additional cost per document: $454.55 x 2= $909.10.

Subsection 8(4) of the Rules provides that, for the purposes of subsections 8(1) to 8(3), the fees are as follows:

Column 1: Approved identity verification facility	Column 2: Base connection amount	Column 3: Amount per kind of document
DVS Hub	Government authority – $5,470.95 Non-government entity – $24,610.40	$454.55
Face Matching Service Hub	Government authority – $12,000 Non-government entity – $31,139.45	$850

A note to subsection 8(4) clarifies that the amounts in the table exclude goods and services tax (GST). Entities may be charged GST where applicable under current taxation policies.[1]

The connection fee is higher for connections to the Face Matching Service Hub than for the DVS Hub because the costs associated with connecting to the technical systems that enable biometric matching through the Face Matching Service Hub are higher.

Column 2 in the tabled at subsection 8(4) of the Rules prescribes the 'base connection amount' for government authorities and non-government entities seeking a new connection to the DVS Hub or Face Matching Service Hub.

The base connection amounts for non-government entities is $24,610.40 for the DVS Hub and $31,139.45 for the Face Matching Service Hub. These amounts seek to recover costs incurred by the department and the external contractor that operates the services on behalf of the Commonwealth (the Managed Service Provider) to onboard new users to the system and establish the technical capability to support electronic communications to and from the approved identity verification facilities.

The base connection amounts for government authorities is $5,470.95 for the DVS Hub and $12,000 for the Face Matching Service Hub. Government authorities would be subject to a lower base connection amount than non-government entities. This is because the connection fee for government authorities only seeks to recover the costs from the Managed Service Provider, noting that the department's costs will be met by funding provided by the Commonwealth.

[1] For further information, see www.ato.gov.au/businesses-and-organisations/gst-excise-and-indirect-taxes/gst.

Column 3 in the table at subsection 8(4) of the Rules prescribes the amount payable by an authority or entity for each 'kind of document' they seek to connect to and be able to request identity verification services using the DVS Hub or Face Matching Service Hub. The amount payable per kind of document is $454.55 for the DVS Hub and $850 for the Face Matching Service Hub.

The cost in column 3 of connecting to new kinds of documents reflects the cost of ensuring the relevant systems can securely and automatically transmit information between the requesting entity and the relevant government databases, and the required system testing.

Importantly, there are no ongoing connection costs. Once an entity is connected to the approved identity verification facility, and irrespective of the number of connections it has to the facility, the entity does not need to pay any ongoing connection costs. However, as discussed above, entities will be subject to additional connection fees if they wish to connect to one or more other kinds of documents (listed at subsection 8(5)), establish a new connection to a facility they are not already connect to, or establish a new connection to a facility they are already connected to.

Connection fees for the NDLFRS have not been provided as entities cannot connect directly to the NDLFRS to request identity verification services.

Subsection 8(5) of the Rules would provide that, for the purposes of subsections 8(2) and (3), each of the following is taken to be a different kind of document:

(a) a birth certificate issued by or on behalf of an authority of a State or Territory;
(b) a death certificate issued by or on behalf of an authority of a State or Territory;
(c) a concession card (within the meaning of the *Social Security Act 1991*);
(d) a notice given under section 37 of the *Australian Citizenship Act 2007* stating that a person is an Australian citizen at a particular time;
(e) a certificate issued by an authority of a State or Territory indicating that an individual has changed the individual's name;
(f) a driver's licence (however described) issued by or on behalf of an authority of a State or Territory;
(g) a document issued by or on behalf of an authority of a State or Territory to assist an individual to prove the individual's age or identity;
(h) a document issued to an individual, as a person who is not an Australian citizen, by the Department administered by the Minister administering the *Migration Act 1958* to assist the individual to prove the individual's identity;
(i) a certificate of marriage issued by or on behalf of an authority of a State or Territory whose function it is to register marriages;

(j) a document issued by a court setting out a divorce order made under the *Family Law Act 1975;*
(k) an Australian travel document (within the meaning of the *Australian Passports Act 2005*);
(l) a certificate signed by an officer (within the meaning of the *Migration Act 1958*) stating that, at a specified time, or during a specified period, a specified person was the holder of a visa that was in effect;
(m) an entry in a Roll (within the meaning of the *Commonwealth Electoral Act 1918*) relating to a particular individual;
(n) an aviation security identification card issued under regulations made for the purposes of the *Aviation Transport Security Act 2004*;
(o) an MSIC issued under regulations made for the purposes of the *Maritime Transport and Offshore Facilities Security Act 2003*;
(p) a medicare card (within the meaning of subsection 84(1) of the *National Health Act 1953*).

The kinds of documents listed at subsection 8(5) reflects current arrangements for the kinds of documents that an authority or entity can seek to be connected to in order to request identity verification services using the facility.

Section 9 – Fees for requests for identity verification services

Section 9 of the Rules would provide the fees payable for each request for identity verification services made by or on behalf of non-government entities and government authorities where a competitive neutrality policy is applicable.

Government authority is defined at section 5 of the Act as 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 Act. A non-government entity is defined at section 5 of the Act to mean a person or body, other than the Commonwealth, a state or territory or a government authority.

Subsection 9(1) of the Rules would provide that, for the purposes of paragraph 42(1)(b) of the Act:

(a) a fee would be payable for a request for an identity verification service mentioned in an item of the table that is made by or on behalf of:
    (i) a government authority, if subsection (2) applies in relation to the request; or
    (ii) a non-government entity; and
(b) the amount of the fee is the amount mentioned in that item

The proposed fee is the same for requests for the DVS and FVS, and is as follows:

Identity verification service	Amount
Document Verification Service	$0.40
Face Verification Service	$0.40

A note to subsection 9(1) clarifies that the amounts in the table exclude goods and services tax (GST). Entities may be charged GST where applicable under current taxation policies.[2]

These fees reflect the costs incurred by government agencies that facilitate the identity verification process, costs from the Managed Service Provider to operate and maintain the services, and the Department's costs to support the management of the services.

Unless a competitive neutrality policy is applicable, requests made by or on behalf of a government authority will not be subject to the fees at section 9. Costs associated with government's use of the services will be met by funding provided by the Commonwealth.

Subsection 9(2) of the Rules would provide that, for the purposes of subparagraph 9(1)(a)(i), this subsection would apply in relation to a request for an identity verification service if:

(a) before the request is made the Department is given notice by or on behalf of the government authority that, taking account of competitive neutrality, it would be appropriate for a fee to be charged for:
    (i) all requests for the service made by or on behalf of the government authority; or
    (ii) particular kinds of requests for the service made by or on behalf of the government authority; and
(b) if subparagraph (a)(ii) applies—the request is of one of the notified kinds.

This provision clarifies that the request fees apply in circumstances where a request made by or on behalf of a government authority relates to business activities that are subject to a Commonwealth, state or territory competitive neutrality policy. This approach ensures compliance with Australia's competitive neutrality policies which seek to prevent government business activities from enjoying a net competitive advantage over their private sector competitors simply by virtue of public sector ownership.

The onus is on the government authority to identify whether a competitive neutrality policy is applicable and to notify the department, if required and necessary. Commonwealth, state and territory government authorities should consider their jurisdiction's competitive neutrality policies for the purposes of subsection 9(2) of the Rules.

[2] For further information, see www.ato.gov.au/businesses-and-organisations/gst-excise-and-indirect-taxes/gst.

At the time of drafting these Rules, the Commonwealth's competitive neutrality policy is *Commonwealth Competitive Neutrality Policy Statement*.

Part 5 – Application, saving and transitional provisions

Section 10 – Application of this instrument as originally made

Subsection 10(1) of the Rules would provide that Part 2, as in force at the commencement of this instrument, would apply in relation to a participation agreement irrespective of whether the agreement is made before, on or after the commencement of these Rules.

As the Act will not commence in its entirety until 14 June 2024, there is currently no requirement for entities that use the services to be a party to a participation agreement. However, subsection 10(1) has been included as some authorities or entities may become a party to a participation agreement prior to commencement of the Act to ensure that essential services can continue to operate without interruptions.

Subsection 10(2) of the Rules provides that Part 3, as in force at the commencement of this instrument, applies in relation to all NDLFRS hosting agreements irrespective of whether the agreement is made before, on or after the commencement of these rules.

This provision is intended to facilitate those state and territory government agencies that choose to become a party to the NDLFRS hosting agreement prior to the commencement of the Act.

Subsection 10(3) of the Rules provides that section 8, as in force at the commencement of this instrument, applies to a connection to an approved identity verification facility made on or after that commencement, whether the request for the connection was made before, on or after that commencement.

This means that entities would be subject to the fees at section 8 if they have sought to be connected to the DVS Hub or Face Matching Service Hub but have not been connected to the relevant facility before 14 June 2024.