Australian Government
Attorney-General's Department

April 2024

Identity Verification Services Rules 2024

This document provides an overview of the draft Identity Verification Services Rules 2024 (the draft Rules), which have been published for public consultation as required under the *Identity Verification Services Act 2023* (IVS Act). This document should be read in conjunction with the draft Rules.

Summary

Subsection 44(1) of the IVS Act provides that the Attorney-General may make rules prescribing matters required or permitted by the Act to be prescribed in the rules, or necessary or convenient to be prescribed for carrying out or giving effect to the Act.

The draft Rules deal with 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 IVS Act:

- listing state and territory privacy laws and government authorities for the purposes of *participation agreements*
- listing state and territory privacy laws for the purpose of the *NDLFRS hosting agreement*, and
- setting fees that government authorities and non-government organisations must pay to connect to, and request the use of, the identity verification services.

Overview of the draft Rules

Part 1: Preliminary

Part 1 of the draft Rules sets out preliminary matters for the rules, including in relation to its commencement.

Clause 2 provides that the Rules will commence on 14 June 2024. The IVS Act in its entirety will also commence on 14 June 2024.[1]

Part 2: Participation agreements

The IVS Act includes important safeguards and protections to ensure access to, and the operation of, the identity verification services does not compromise the privacy of Australians and the security of information. This ensures the Australian community can have confidence that an individual's personal and sensitive information will be protected when used to verify their identity.

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

[1] Section 2 of the IVS Act provides that all remaining provisions in the Act will commence the earlier of the commencement of the rules or 6 months after the Act received Royal Assent, which occurred on 14 December 2023.

Commonwealth.[2] All entities seeking to make a request for identity verification services must be a party to a participation agreement[3] and meet the privacy obligations and requirements set out in the IVS Act.

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

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

Clause 5 of the draft Rules prescribes the following list of state and territory privacy laws for the purpose of paragraph 9(1)(b) of the IVS Act:

- *the Privacy and Personal Information Protection Act 1998* (NSW)
- *the Privacy and Data Protection Act 2014* (Vic)
- *the Information Privacy Act 2009* (Qld)
- *the Personal Information Protection Act 2004* (Tas)
- *the Information Privacy Act 2014* (ACT)
- *the Information Act 2002* (NT)

By prescribing these privacy laws, the draft Rules will enable all entities that are subject to these laws, including relevant state and territory government agencies, to become a party to a participation agreement.

The rules will 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 IVS Act in order to become a party to a participation agreement. This includes being subject to the *Privacy Act 1988* (Cth) or agreeing to comply with the Australian Privacy Principles.

Clause 6 of the draft Rules prescribes the following government authorities for the purpose of paragraph 9(1)(d) of the IVS Act:

- the Australian Criminal Intelligence Commission
- the Australian Secret Intelligence Service
- the Australian Security Intelligence Organisation
- the National Anti-Corruption Commission, and
- the Office of National Intelligence.

It is necessary and appropriate to prescribe these Commonwealth integrity and intelligence agencies as they have a demonstrated operational need to use the identity verification services but cannot satisfy another requirement in subsection 9(1). This is because they are exempt from complying with the Privacy Act and the Australian Privacy Principles.

Despite being exempt from the Privacy Act, these Commonwealth agencies will be subject to the privacy safeguards and obligations in the IVS Act in relation to their use of the identity verification services. This includes: notification requirements relating to security breaches, privacy impact assessments and requirements to comply with obligations relating to the use and disclosure of information obtained through the identity verification services. These Commonwealth agencies also have appropriate privacy rules and safeguards in place, and are subject to independent oversight and scrutiny.

[2] See section 8 of the IVS Act for the definition of participation agreement.
[3] See paragraph 15(1)(b) of the IVS Act for the Document Verification Service, paragraph 19(a) for the Face Verification Service, and paragraph 17(1)(a) for the Face Identification Service.

As a result of **subclause 10(1)** of the draft Rules, Part 2 would apply in relation to all participation agreements irrespective of whether the agreement is made before, on or after the commencement of these rules.

As the IVS Act has not commenced in its entirety, there is currently no requirement for entities that use the services to be a party to a participation agreement. However, subclause 10(1) has been included as some entities may become a party to a participation agreement prior to commencement to ensure that essential services can continue to operate without interruptions.

Part 3: NDLFRS hosting agreements

The National Driver Licence Facial Recognition Solution (the NDLFRS) is an electronic database of state and territory identity documents (such as driver's licenses), and systems and templates that enable identity verification to occur against facial images in the database.[4]

The NDLFRS will enable Australians to use a state or territory issued driver's licence to biometrically verify their identity via the Face Verification Service. Biometric verification is required to create a digital ID with a higher level of assurance, such as a 'strong' myGovID.

Currently, only Australians with a passport can biometrically verify their identity, accounting for approximately 50 per cent of the population. As approximately 80 per cent of the population have a driver's licence, the NDLFRS will enable more Australians to biometrically verify their identity and access critical government services.

The IVS Act sets out security measures and obligations to protect personal information stored on the NDLFRS, which are reflected in the *NDLFRS hosting agreement*.[5] 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.

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 IVS Act. Of relevance to Part 3 of the draft Rules, these require a government authority that is a party to the agreement to be subject to a state or territory privacy law that is prescribed in the rules.

Clause 7 of the draft Rules prescribes the following list of state and territory privacy laws for the purpose of paragraph 13(2)(a) of the IVS Act:

- *the Privacy and Personal Information Protection Act 1998* (NSW)
- *the Privacy and Data Protection Act 2014* (Vic)
- *the Information Privacy Act 2009* (Qld)
- *the Personal Information Protection Act 2004* (Tas)
- *the Information Privacy Act 2014* (ACT)
- *the Information Act 2002* (NT)

South Australian and Western Australian laws are not included as these jurisdictions do not currently have privacy laws in force. Government agencies will need to satisfy another requirement at subsection 13(2) of the IVS 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.

[4] See section 5 of the IVS Act for the definition of the NDLFRS.
[5] See subsection 13(1) of the IVS Act for the definition of the NDLFRS hosting agreement.

As a result of **subclause 10(2)** of the draft Rules, Part 3 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 IVS Act.

Part 4: Fees

Part 4 of the draft Rules provide:

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

The proposed fees align with, and are authorised by, section 42 of the IVS Act.

Clause 8 - Connection fees

Clause 8 provides for the fees to connect to the approved identity verification facilities and how they apply. 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 organisation – $24,610.40	$454.55
Face Matching Service Hub	Government authority – $12,000 Non-government organisation – $31,139.45	$850

Note: These amounts exclude goods and services tax (GST). Entities may be charged GST where applicable under current taxation policies.[6]

How do connection fees work? How do they apply?

The application of connection fees will vary depending on whether an entity is already connected to an approved identity verification facility and the number of document types or 'kinds of documents' (listed at subclause 8(5)) an entity intends to use to make requests for the identity verification services.

Subclause 8(2) provides that an entity connecting for the first time to an approved identity verification facility would be subject to:

- the one-off 'base connection amount' (column 2) that is relevant to the facility, **and**
- the additional amount in column 3 for each kind of document (listed at subclause 8(5)) in relation to which the entity is seeking to be able to request identity verification services using the facility.

An entity that is connected to one approved identity verification facility and seeks to connect to the other facility would also be subject to the requirements set out at subclause 8(2).

Subclause 8(3) provides for how the fees apply to those entities that are already connected to the approved identity verification facility but seek to be connected to that facility in relation to additional kinds of documents listed at subclause 8(5). In this circumstance, the 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

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

services using the facility. The entity would not be required to pay an additional 'base connection amount' as it is are already connected to the facility.

The examples below clarify the application of connection fees.

Example – First time connection to the approved identity verification facility

A non-government organisation seeks to connect to the Face Matching Service Hub. The organisation intends to make requests for the Face Verification Service using Australian passports and driver's licences, which are two kinds of documents listed at subclause 8(5). This organisation 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 organisation would pay a total one-off connection fee of $32,839.45 (excl GST).

Example – An entity seeking to connect to additional documents

A non-government organisation 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 two documents – driver's licences and Medicare cards. The organisation would pay the following one off connection fees:

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

Example – A Commonwealth department connecting to a facility

A Commonwealth department is seeking to connect to the DVS hub and intends to make requests for the Document Verification Service using driver's 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 (for further information, see the section below ***How have the connection fees been calculated?***).

Example – Connecting to both approved identity verification facilities

A non-government organisation seeks to connect to the DVS hub and intends to make requests for the Document Verification Service using Medicare cards, change of name certificates and birth certificates.

The organisation also seeks to connect to the Face Matching Service Hub and intends to make requests for the Face Verification Service using Australian passports and driver's licences.

This organisation 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 organisation would pay a total one-off connection fee of $58,813.5 (excl GST).

Are there any ongoing connection costs?

No. Once an entity is connected to the approved identity verification facility, it does not need to pay any ongoing connection costs. However, as discussed above, entities will be subject to additional connection fees should it wish to connect to additional kinds of documents (listed at subclause 8(5)) or to a facility to which it is currently not connected.

How have the connection fees been calculated?

The 'base connection amount' (column 2) for non-government organisations seeks 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.

Government authorities would be subject to a lower 'base connection amount' than non-government organisations. 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.

The connection fee is higher for connections to the Face Matching Service Hub than for the Document Verification Service hub because the costs associated with connecting to the technical systems that enable the Face Matching Service Hub are higher.

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.

When do connection fees apply?

As provided by subclause 10(3) of the draft Rules, Part 4 applies to connections to the approved identity verification facilities that occurs on or after the commencement of these rules, irrespective of when the request to connect was made.

This means that entities would be subject to the fees at clause 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.

Clause 9 – Request fees

Clause 9 of the draft Rules provides for the fees payable for each request for identity verification services that is made by or on behalf of non-government organisations and government authorities where a competitive neutrality policy is applicable.

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

The proposed fee is the same for requests for the Document Verification Service and the Face Verification Service, and is as follows:

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

Note: These amounts exclude GST. Entities may be charged GST where applicable under current taxation policies.[7]

When do the request fees apply?

The request fees will apply from the commencement of these rules (14 June 2024).

Application of request fees to government authorities

Subclause 9(2) 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 seeks to prevent government business activities from enjoying a net competitive advantage over their private sector competitors simply by virtue of public sector ownership.

If a competitive neutrality policy is applicable, the department is to be given a notice by or on behalf of the government authority stating that it would be appropriate to charge a fee for:

- all requests for the service made by or on behalf of the government authority; or
- particular kinds of requests for the service made by or on behalf of the government authority.

The onus is on the government authority to identify whether a competitive neutrality policy is applicable. Commonwealth, state and territory government authorities should consider their jurisdiction's competitive neutrality policies for the purposes of subclause 9(2) of the draft Rules.[8]

How have the connection fees been calculated?

The request fee reflects 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.

[7] For further information see www.ato.gov.au/businesses-and-organisations/gst-excise-and-indirect-taxes/gst.
[8] The Commonwealth's competitive neutrality policy can be found on the Department of Treasury's website (www.treasury.gov.au/publication/commonwealth-competitive-neutrality-policy-statement).