Australian Government
Attorney-General's Department

2 October 2023

Senate Legal and Constitutional Affairs Legislation Committee

Inquiry into the Identity Verification Services Bill 2023 and the Identity Verification Services (Consequential Amendments) Bill 2023

Attorney-General's Department Submission

Contents

Introduction

1. The Attorney-General's Department (the Department) welcomes the opportunity to provide a submission to the Senate Legal and Constitutional Affairs Legislation Committee's *Inquiry into the Identity Verification Services Bill 2023 and the Identity Verification Services (Consequential Amendments) Bill 2023*.
2. The Identity Verification Services Bill 2023 (IVS Bill) and the Identity Verification Services (Consequential Amendments Bill) 2023 (Consequential Amendments Bill) were introduced into the Australian Parliament by the Attorney-General, the Hon Mark Dreyfus KC MP, on 13 September 2023.
3. The IVS Bill provides clear legislative authority for the identity verification services and ensures the services operate subject to strong privacy safeguards, oversight and transparency arrangements. The identity verification services are a critical capability provided by the Commonwealth and are used every day by government and industry to verify the personal information on a passport, driver's licence, birth certificate or other government issued credential.
4. The IVS Bill addresses the recommendations made by the Parliamentary Joint Committee on Intelligence and Security in its inquiry into the Identity-matching Services Bill 2019. As recommended by the Parliamentary Joint Committee, the Bill aligns with the following principles:
    - the regime is built around privacy, transparency and subject to robust safeguards
    - privacy obligations and safeguards are required by the IVS Bill and will be implemented in practice through a participation agreement
    - the regime is subject to Parliamentary oversight and reasonable, proportionate and transparent functionality, and
    - annual reporting requirements for the identity verification services are included.
5. The IVS Bill is supported by the Consequential Amendments Bill, which amends the *Australian Passports Act 2005* (Cth) and ensures personal information on an Australian travel document, such as an Australian passport, can be disclosed for the purpose of sharing or matching information relating to the identity of a person.
6. The IVS Bill and Consequential Amendments Bill will ensure that industry, government and the community can continue to benefit from safe, secure and private identity verification through the services.
7. The Department has consulted the following Commonwealth agencies on this submission:
    - the Australian Federal Police
    - the Department of Finance
    - the Department of Social Services
    - the Student Identifiers Registrar, and
    - the Australian Transaction Reports and Analysis Centre.

Overview of the identity verification services

8. Secure and efficient identity verification protects the privacy of Australians and is vital to the digital economy. It ensures that Australians can access critical government and industry services and decreases the risk of identity crime.

9. The identity verification services are a series of automated services that are used to compare the personal information on a person's identification document (such as an Australian passport or driver's licence) against Commonwealth, state and territory government records. These services are offered by the Commonwealth and provide the only national capability for industry and government to securely and efficiently verify the identity of their customers.

10. The services that make up the identity verification services are:

    - the Document Verification Service and Face Verification Service, which are 1:1 matching services, and
    - the Face Identification Service, which is a 1:many matching service.

Background

11. The operational need for a national capability to support identity verification was identified by the Council of Australian Governments (COAG) at a Special Meeting on Counter-Terrorism on 27 September 2005. At that meeting, COAG agreed to the development and implementation of a national document verification service to combat identity theft and fraudulent use of stolen and assumed identities.

12. To implement the COAG agreement and establish a national approach for the use of the identity verification services, Commonwealth, state and territory governments entered into the *Intergovernmental Agreement on Identity Matching Services* (Intergovernmental Agreement) on 5 October 2017.

13. The Intergovernmental Agreement established a common understanding of the roles and responsibilities of the Commonwealth, states and territories in operating and using the identity verification services. It also supported the provision of data holdings for the identity verification services and established clear safeguards and oversight arrangements to protect the privacy of Australians.

14. Key events in the operation and use of the identity verification services are summarised below:

    - Government use of the Document Verification Service commenced in 2008.
    - In 2014, the Document Verification Service was expanded to enable industry use of the service, subject to privacy safeguards and protections.
    - The Face Verification Service commenced in 2016 for transactions by government agencies only.
    - The Face Identification Service has been used on three occasions between 2018 and 2021, in limited trials and pilot programs by state police.

Current uses

15. The identity verification services are a foundational capability to the Australian economy and are used extensively by government and industry to securely verify the identity of their customers. In 2022, the Document Verification Service was used over 140 million times by approximately 2700 public and private

sector organisations. In the 2022-23 financial year, there were about 2.6 million transactions of the Face Verification Service by government agencies

16. The identity verification services are embedded within the day-to-day operations of government and industry, and support Australians to access the services they need. Of particular significance, the identity verification services are relied upon to verify the identity of Australians when seeking to establish a myGovID in order to access Centrelink, Australian Taxation Office services and other critical services. Over 11.3 million myGovIDs have been created using the Document Verification Service. Around one third of these have been biometrically verified against information on a person's Australian passport, using the Face Verification Service which provides a higher level of verification. A higher level of identity verification allows a person to use their Digital ID to access services that have a higher level of identity risk, such as applying for a tax file number online.

17. Other examples of government and industry use of the identity verification services are provided below.

Example 1 – 'Know Your Customer' obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)

18. The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) aims to prevent money laundering and the financing of terrorism by imposing a number of obligations on the financial sector, gambling sector, remittance (money transfer) services, bullion dealers and other professionals or businesses (known as 'reporting entities') that provide particular services (known as 'designated services').

19. One of the core AML/CTF obligations is the requirement to undertake customer due diligence. To meet this requirement, the AML/CTF Act requires reporting entities to undertake customer identification (know your customer) procedures. These procedures reflect the obligations in the AML/CTF Act for reporting entities to collect 'know your customer' information about their customers and beneficial owners, and verify it using independent and reliable documentation or electronic data (or both). Reporting entities must document the procedures they use in their AML/CTF Program.

20. To assist reporting entities with meeting their obligations, the Australian Transaction Reports and Analysis Centre promotes the use of the Document Verification Service in its guidance as a secure option for verifying individual customer and beneficial owner identification using electronic data. The Document Verification Service is widely used by reporting entities for this purpose and enables them to check in real time that the document is current and not lost or stolen.

Example 2 – Verifying identity for social security payments

21. Individuals making a claim for social security payment through Services Australia must meet an identity proofing standard. The standard involves identity confirmation and verification as provided by section 8 of the *Social Security (Administration) Act 1999* (Cth).

22. The Document Verification Service allows individuals to meet these identity proofing standards and, accordingly, supports with the provision of social security payments. In May 2023, almost 90,000 documents were successfully verified through the Document Verification Service.

Example 3 – developing and maintaining a Unique Student Identifier

23. As part of administering the Unique Student Identifier initiative under the *Student Identifiers Act 2014* (Cth), the Office of the Student Identifiers Registrar uses the Document Verification Service to verify identity documents when creating a Unique Student Identifier or updating personal details. Each week,

the Document Verification Service is used in the creation of approximately 26,000 Unique Student Identifiers and for 12,000 transactions to update details.

24. Issuing and maintaining a Unique Student Identifier is required for:

    - all students undertaking Nationally Recognised Training in Australia;
    - all students undertaking Higher Education in Australia;
    - all students applying for tertiary support such as HECS-HELP;
    - an education or training provider to issue a statement of attainment or a qualification; and
    - an education or training provider to report training or education outcomes such as to the National VET collection.

Digital ID and the identity verification services

25. The IVS Bill will support the Australian Government's priorities in developing a whole-of-economy Digital ID system. The Government's Digital ID system will enable Australians to prove their identity online in secure, convenient, voluntary and inclusive ways when accessing services. On 19 September 2023, the Minister for Finance, Senator the Hon Katy Gallagher, released an exposure draft of the Digital ID Bill 2023 which will legislate and strengthen a voluntary accreditation scheme for Digital ID service providers operating across the economy. It will also provide legislative authority to expand the Australian Government Digital ID System to include a broader range of government and private sector entities that choose to participate in the system.

26. The identity verification services provide the enabling capability to create a Digital ID and will play a critical role in its ongoing roll out in Australia. This is because the Document Verification Service and Face Verification Service will be used by *accredited providers* (as defined under the Digital ID Bill 2023) to verify the identity of a person seeking to create a Digital ID. The automated nature of the Document Verification Service and Face Verification Service means that accredited providers will receive an instant result which will support the efficient and secure creation of Digital IDs.

27. Currently, around 50 per cent of Australians can choose to biometrically verify their identity. By establishing the National Driver Licence Facial Recognition Solution (discussed in detail below), the IVS Bill will also enable the approximately 80 per cent of Australians with a driver's licence to have their identity biometrically verified and create a Digital ID to a higher level of assurance.[1] This standard of Digital ID will be needed by those individuals seeking to access services which necessitate a higher level of verification (such as welfare payments).

Outline of the Identity Verification Services Bill

What is the purpose of the IVS Bill

28. The IVS Bill will provide clear legislative authority for the identity verification services to operate subject to strong privacy safeguards and limitations enshrined in law. It will provide clarity and transparency as to the purposes and use of the identity verification services, and ensures that the continued operation of the services are subject to strong oversight and transparency arrangements. This will give the Australian

[1] The Australian Government's Trusted Digital Identity Framework provides more information on identity proofing levels and the standards or requirements for creating a Digital ID to a higher level of assurance.

community certainty that their personal information will be protected when government and industry use the services to verify identity.

29. The need to legislate for the identity verification services is more important today than ever before. The identity verification services are a foundational capability to the Australian economy and are used every day by governments and industry. The services will become even more crucial to the provision of government and industry services as the voluntary accreditation scheme for Digital ID service providers (to be strengthened by the Digital ID Bill 2023) expands across the economy.

30. In addition to providing for the identity verification services, the IVS Bill will regulate the Department's use and operation of the *approved identity verification facilities*[2] which provides the technical capability for a request to be made for an identity verification service, and enables the operation of the National Driver Licence Facial Recognition Solution.

31. By legislating for the identity verification services, the IVS Bill ensures the Australian community can benefit from the continued operation of the services which supports the secure and efficient verification of identity for access to critical services. For example, it will ensure that Australians can have their identity verified with their consent when seeking access to welfare payments, opening a bank account and creating a tax file number.

32. The identity verification services are a beneficial service to the Australian community, and will support broader efforts to prevent identity crime. The Document Verification Service and Face Verification Service are used extensively by government and industry because they offer the only national capability to securely verify the identity of Australians with the individual's consent.

33. The IVS Bill ensures that the identity verification services are used in accordance with privacy law and principles, and subject to other privacy safeguards and protections which includes (but is not limited to): consent requirements, complaints handling mechanisms, requirements to report security and data breaches, privacy impact assessments, and limitations on the collection, use and disclosure of information. There are also extensive oversight and transparency arrangements in the IVS Bill including (but not limited to): annual reporting, annual assessments by the Information Commissioner, compliance auditing requirements, and the publishing of agreements and access policies.

34. This ensures the ethical and appropriate use of the identity verification services, and prevents the services from being used for general law enforcement purposes, intelligence gathering, or mass surveillance. The IVS Bill and the provision of the identity verification services will be subject to a statutory review within 2 years of its commencement to ensure the operation of the services and the privacy safeguards and protections remain appropriate.

35. The IVS Bill does not regulate the use of biometric information and identity matching undertaken outside of the identity verification services. The broader use of facial recognition by government, or matching against non-government issued identification documents is not within the scope of the IVS Bill. Furthermore, the IVS Bill does not provide for the regulation of the commercial use of biometric technology, such as facial recognition, by the private sector.

36. The regulation of biometric information is being considered by all governments. On 22 September 2023, the Standing Council of Attorneys-General discussed the risks and benefits associated with the

[2] *Approved identity verification facility* is defined at clause 5 and includes the *DVS Hub*, the *Face Matching Service Hub* and the *NDLFRS*

development and use of facial recognition and biometrics and agreed that the risks warrant a coordinated national response. This will include consideration of the adequacy of regulation to ensure the risks are appropriately addressed. The Standing Council will discuss future regulatory approaches before the end of 2023 and the Australian Government will provide an update on the progress of other relevant initiatives, including broader privacy reform, the Australian Government Digital ID system and the National Strategy for Identity Resilience.

37. On 28 September 2023, the Australian Government released its response to the Privacy Act Review. The response acknowledges that certain types of personal information-handling, such as facial recognition technology and other uses of biometric information, pose higher privacy risks to individuals. The Government agreed in-principle that non-government entities should be required to conduct a Privacy Impact Assessment for activities with high privacy risks.[3] A Privacy Impact Assessment is a systematic assessment of a project that identifies potential privacy impacts and recommendations to manage, minimise or eliminate them.[4]

38. The Government response agreed that further consideration should be given to enhanced risk assessment requirements in the context of facial recognition technology and other uses of biometric information and that the Office of the Australian Information Commissioner should continue to develop guidance for new technologies.

Scope of the IVS Bill

39. The IVS Bill will support the efficient and secure operation of identity verification services while ensuring strong standards of privacy. In particular the IVS Bill will:

    - authorise government and industry to make a request for the Document Verification Service (DVS) and Face Verification Service (FVS) – which are 1:1 matching services – for the purpose of identity verification
    - provide for the National Driver Licence Facial Recognition Solution (NDLFRS) which will facilitate the 1:1 matching of identity. In particular, the NDLFRS enables the FVS to conduct 1:1 matching against driver's licences, and ensures more Australians can create Digital IDs
    - authorise limited government agencies to make requests for the Face Identification Service (FIS) – a 1:many matching service – for the purpose of protecting the identity of a *shielded person*, such as undercover officers and protected witnesses. 1:many matching through the identity verification services will not be authorised for other purposes and will therefore be prohibited, and
    - authorise the responsible Commonwealth department – the Attorney General's Department – to develop, operate and maintain the facilities needed to support the operation of identity verification services.

40. As discussed in detail below, the IVS Bill includes robust safeguards and limitations to protect the privacy of Australians. This ensures that the operation of the approved identity verification facilities and requests for the identity verification services are subject to privacy safeguards, security measures, and oversight and transparency arrangements.

---

[3] This is a requirement of the IVS Bill, see subclause 9(2). Note, Australian Government agencies must conduct a PIA for all high privacy risk projects as required by the Privacy (Australian Government Agencies – Governance) APP Code 2017.
4 OAIC, *Privacy impact assessments* (Web Page, 29 September 2023)

1:1 matching – The Document Verification Service and Face Verification Service

41. The IVS Bill will enable 1:1 matching of identity through a DVS and FVS.

    - A DVS enables the verification of biographic information (such as a name, date of birth, address etc) against government issued identification documents.
    - A FVS enables the verification of biometric information (in this case a photograph or facial image of an individual) against a government issued identification documents.

42. Government and industry entities that are a party to a *participation agreement* (as defined at clause 8 and discussed below) will be authorised to make a DVS and/or FVS request for the purpose of verifying the identity of a person with their consent. Certain government agencies will also be authorised to make a FVS request for the purpose of protecting the identity of a *shielded person* (as defined in clause 5 and discussed below).

43. In response to a DVS request, entities will receive a either a statement that the information compared matched, or a statement that the information compared did not match (with or without reasons why there was no match). The type of response is not dependent on the type of entity making the request (subclause 15(1)(g)).

44. A FVS will provide different types of functionality depending on what entity is requesting the service. Non-government entities will only receive a 'match' or 'no match' response (see subclause 19(d)), whereas government entities may also receive additional information about an individual such as the person's image on the government identification document.

45. The hypothetical example below provides further clarity of the intended operation of 1:1 matching through the identity verification services.

> **Hypothetical example – DVS request by a non-government entity**
>
> 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 (which is an *approved identity verification facility)* 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.

National Driver Licence Facial Recognition Solution

46. The operation of the identity verification services, specifically the DVS and FVS, will be facilitated through the NDLFRS, which consists of:

- an electronic database of information on state and territory identity credentials (currently driver's licence information), and
- the technical systems and templates used to enable identity verification to occur against facial images in the database.

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

48. 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. This will allow Australians with a driver's licence to create a Digital ID to a higher level of assurance. If passed, the Digital ID Bill will enable accredited Digital ID providers to offer Australians the choice to verify themselves biometrically. Australians who choose to use their secure Digital ID to access services will, in doing so, reduce their risk of identity theft and fraud.

49. The NDLFRS is operated and maintained by the Commonwealth on behalf of all jurisdictions, consistent with the Intergovernmental Agreement. The operation of the NDLFRS is also supported by state and territory law as most jurisdictions have passed legislation or amended subordinate legislation to allow for the uploading of information on identity credentials to the database.

50. Currently, Tasmania, Victoria and South Australia have uploaded their jurisdiction's data into the NDLFRS. However, the NDLFRS cannot yet be used for identity verification purposes and will not be accessible until after the passage and commencement of the IVS Bill. This will ensure that the use and operation of the NDLFRS for the purposes of the DVS and FVS is subject to the privacy safeguards and limitations in the IVS Bill. The Department anticipates that further jurisdictions will provide their data for use on the NDLFRS in the near future.

1:many matching – Face Identification Service

51. A 1:many matching service compares a facial image (such as a photograph) against other facial images across government records. The FIS is a 1:many matching service. This type of matching differs from 1:1 matching services (such as the DVS and FVS) which matches particular biometric or biographic information against a particular record, rather than many.

52. 1:many matching through the FIS is a critical service that can be used to confirm that the true identity or a previous assumed identity of a *shielded person* is protected and cannot be used for verification purposes through the DVS or FVS. A shielded person is defined in clause 5 and covers persons with a legally assumed identity (such as undercover officers and protected witnesses) which has been obtained under a Commonwealth, state or territory law (including Part IAC of the *Crimes Act 1914* (Cth) and the *Witness Protection Act 1994* (Cth)).

53. It is essential for law enforcement to be able to make a request for the FIS to ensure they can carry out their functions in protecting shielded persons. Without this capability, there is a real risk that a nefarious actor could lawfully verify the identity of a shielded person through a DVS or FVS request. This could compromise the safety and security of a shielded person and their family, and undermine a law enforcement or national security investigation.

54. The below hypothetical example demonstrates how the use of the FIS can protect the identity of shielded persons.

> **Hypothetical example – use of the FIS to protect a shielded person**
>
> 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 and other identification information to be searched across data holding agencies to determine if the undercover officer has a government identification document (like a licence) under their true identity or a different identity which may have been used in a previous undercover operation.

55. The IVS Bill includes a number of important limitations to ensure the use of the FIS occurs appropriately and only when needed to protect the identity of shielded persons. These limitations are in addition to the safeguards and protections for making a request for an identity verification service which includes the requirement for a participation agreement to be in place.

56. Limitations in relation to the FIS are discussed below:

Permitted purposes

57. A FIS request can only be made for the purpose of protecting an individual who is a shielded person, or someone else associated with a shielded person (subclause 18(3)). This is an important limitation and provides certainty that the FIS will not be used for general law enforcement and intelligence purposes, or mass surveillance.

Limitations on access to the FIS

58. As noted above, a FIS request can only be made by limited government agencies that administer or have authority to acquire or use a legally assumed identity under an existing law, for example the Crimes Act or Witness Protection Act (subclause 17(1)). This includes certain Commonwealth, state and territory law enforcement and national security agencies, and anti-corruption agencies. Other government agencies and private sector organisations will not be able to make a FIS request.

59. This ensures the FIS is only used by those government entities with an operational need to manage and protect shielded persons, and their associates.

Authorisation of a FIS request

60. The IVS Bill provides robust and proportionate requirements for the authorisation of a FIS request which ensures the service is only used for the purpose of protecting the identity of a shielded person, and not for intelligence or surveillance purposes.

61. This authorisation process is summarised below:

- a FIS can only be requested by an officer on behalf of a government authority listed in subclause 17(1) for the purpose of protecting the identity of a shielded person or someone else associated with a shielded person (subclause 17(1)(b))
- the officer must be approved as a suitable person to make the request (or requests of that kind) by the head of the government authority or senior management (subclause 17(2))

- the request must have specific characteristics and include a single facial image of an individual (subclause 17(3))
- the request must be endorsed by a senior officer of the same government authority (subclause 17(4)), and
- a person must not endorse a request 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)).

62. This authorisation process will ensure requests made for a FIS are appropriate and subject to senior level oversight.

Facilities to operate the identity verification services

63. The IVS Bill will authorise the Attorney-General's Department to operate the facilities needed for the effective operation of the identity verification services. These facilities are defined as *approved identity verification facilities* in the IVS Bill and consist of the *DVS Hub*, *Face Matching Service Hub* and the *NDLFRS*.

64. 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, as discussed in detail below.

65. The below hypothetical example demonstrates how these facilities operate:

Hypothetical example – use of the DVS Hub

A Commonwealth agency is seeking to make a DVS request in order to verify the identity of a customer (with their consent). The Commonwealth agency submits a DVS request with information from the customer's passport, including biographic information and the passport number. The request will be sent to the DVS Hub which then automatically routes the request to the Australian Passport Office. The information in the request is matched against the information held in the data holdings of the Australians Passport Office. This matching process occurs at the data source (i.e. the Australian Passport Office). A 'match' or 'no match' result is returned to the Commonwealth agency through the DVS Hub.

Privacy safeguards and security protections

66. The IVS Bill includes a number of 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 should provide the Australian community with confidence that an individual's personal and sensitive information will be protected when used to verify their identity or stored in a database on the NDLFRS.

67. These privacy safeguards will be reflected in *participation agreements* (defined in clause 8) between the relevant entity and the Department (representing the Commonwealth). This will ensure that entities have signed an agreement demonstrating their intent to be bound by these privacy obligations and

requirements when making a request for identity verification services. All entities seeking to make a request for the identity verification services must be a party to the participation agreement.

68. Similarly, the operational requirements and security measures in relation to the NDLFRS are reflected in the *NDLFRS hosting agreement* (as defined in clause 13). 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.

Compliance with privacy law or obligations

69. In order to make a request for an identity verification service, entities must be a party to a participation agreement and satisfy one of the following (subclause 9(1)):

- be subject to the *Privacy Act 1988* (Cth). The Privacy Act applies to Ministers, Departments, a range of Commonwealth agencies and organisations that are not small businesses operators (see sections 6, 6C and 6D of the Privacy Act).
- be subject to a privacy law of a state or territory, where that law is prescribed in the rules. The application of these laws varies, but generally includes state or territory agencies such as road authorities.
- have agreed to comply with the Australian Privacy Principles as if the entity were an 'APP entity' within the meaning of section 6 of the Privacy Act. This would apply to:
    - 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
- the entity is a government authority prescribed by the Minister in the rules**.** This would allow Commonwealth government authorities that are exempt from the Privacy Act to be parties to participation agreements, such as the Australian Security Intelligence Organisation, Australian Secret Intelligence Service, Australian Signals Directorate and Office of National Intelligence. If state or territory government authorities were unable to comply with Australian Privacy Principles as an 'APP entity', this would also provide an avenue for them to become party to a participation agreement, or
- be an authority, person or body subject to the *Privacy Act 1993* (NZ). 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 similar New Zealand services. Importantly, New Zealand based entities will not be able to make a request for any other services (see subclause 19(a)).

70. Similarly, for the purposes of the NDLFRS, relevant government authorities must be subject to a Commonwealth, state or territory privacy law, or agree to be bound by the privacy obligations under the Australian Privacy Principles (subclause 13(2)).

Consent and access to personal information

71. The IVS Bill requires participation agreements to provide for the obtaining of a person's informed consent to the collection, use and disclosure of *identification information*[5] when requesting an identity verification service (subclause 9(2)(b)).

72. When obtaining consent, entities must notify individuals of certain matters (subclause 9(3)). This supports a person to provide informed consent, after considering key matters, including:

    - how the entity seeking consent uses identity verification services and how any facial images collected by that entity for the purpose of making a request for services will be used and disposed of (subclause 9(3)(a) and (b)
    - whether facial images will be retained for any other purposes (subclause 9(3)(c))
    - what legal obligations the entity 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)), and
    - where the individual can get information about making complaints (subclause 9(3)(d)), and where the individual can get information about the operation and management of the approved identification verification facilities (subclause 9(3)(h)).

73. 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 identification information is:

    - for the purposes of protecting a shielded person, or someone else associated with a shielded person, and
    - implicit in functions conferred by law on the authority.

74. This reflects that it may not always be possible for officers listed at subclause 17(1) to obtain consent when making a FVS or FIS request to protect the identity of a shielded person or someone else associated with a shielded person.

75. For example, there may be a need for an authority to make a FVS request years after a person has obtained an assumed identity under Part IAC of the Crimes Act 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.

76. The IVS Bill ensures that individuals can have access to their information and have any errors corrected. In particular, the NDLFRS hosting agreement requires state and territory government authorities to:

    - take reasonable steps to inform each individual that their identification information is, or is to be, included in a database in the NDLFRS (paragraph 13(3)(a)), and

[5] *Identification information* is defined at clause 6 and includes *personal information* and certain types of *sensitive information* as defined under the Privacy Act.

- 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 13(3)(b)).

Limitations and protections for the collection, use and disclosure of personal information

77. The IVS Bill provides legislative authority for the Department to collect, use and disclose identification information that has been communicated to an approved identity verification service, or generated using the NDLFRS. This means, for example, the Department may collect identification information (such as biographic information on a driver's licence) from a state or territory authority for the purposes of developing the NDLFRS.

78. The authority for the Department to collect identification information is limited to the purposes outlined in subclause 27(2):

    - 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 the services above, or
    - developing, operating or maintaining the NDLFRS.

79. Subclauses 27(3), (4) and (5) supports subclause 27(1) by clarifying the methods that are authorised for the collection of identification information.

80. Subclause 28(1) 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, or
    - held in, or generated using, the NDLFRS.

81. These important limitations are intended to ensure that identification information, including personal information and sensitive information, generated under the IVS Bill is not collected, used or disclosed for purposes unrelated to the identity verification services. This reflects the Department's role under the IVS Bill which is intended to be limited to facilitating the operation of, and supporting the making of requests for, the identity verification services.

82. Subclauses 30(1) and (2) further protect personal information through the provision of criminal offences for current and former *entrusted persons*[6] who record, disclose or access *protected information*[7]. The maximum penalty for the offences would be imprisonment for 2 years. This penalty reflects the serious consequences that may arise from the relevant conduct, given that a breach of the obligations of entrusted persons may place a person's life or safety at risk.

---

[6] *Entrusted person* is defined at subclause 30(4) of the IVS Bill, and includes: the Secretary of the Department, APS employees of the Department, a person whose services are made available to the Department, and a contractor engaged to provide services to the Department in connection with an approved identity verification facility.
[7] *Protected information* is defined at subclause 30(4) of the IVS Bill.

83. Clause 30 creates specific exceptions to these criminal offences 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, or
    - the conduct is in compliance with a requirement under a law of the Commonwealth or of a state or territory.

84. The exceptions to subclauses 30(1) and (2) apply in addition to the authorisations set out in clauses 31, 32, 33, 34, and 35 of the IVS Bill which ensures that an entrusted person will not be inappropriately subject to criminal liability for their conduct where:

    - 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 protection 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.

85. These exceptions reflect that the criminal offences at 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 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. The exceptions are also intended to support the oversight functions of the IGIS and Ombudsman, and permit the disclosure of protected information where necessary to protect lives or with consent.

Privacy impact assessment

86. Subclause 9(2)(a) requires participation agreements to provide for *privacy impact assessments* of requesting identity verification services.

87. The IVS Bill defines privacy impact assessment to have the same meaning as in subsection 33D(3) of the Privacy Act. 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.

Complaints handling processes

88. Subclause 9(2)(d) requires parties to the participation agreement to establish and maintain a mechanism to deal with complaints from individuals whose identification information is held by the entity. Similarly, subclause 13(3)(d) requires state and territory government authorities to have a means for dealing with complaints by individuals relating to their information on the NDLFRS.

89. These requirements will ensure individuals have an appropriate avenue to pursue any complaints directly with the entity or government authority. Other relevant Commonwealth, state and territory complaints handling mechanisms will continue to be available, including those provided by the Commonwealth Ombudsman and the OAIC under section 36 of the Privacy Act.

Security protections

90. The IVS Bill places a number of obligations on the Department to maintain the security of the approved facilities and protect the personal information of Australians.

91. The Department is required to use encryption and do anything else necessary to maintain the security of electronic communications to and from the approved identity verification facilities and information held in databases in the NDLFRS (subclauses 13(4) and 25(a)). The IVS Bill does not prescribe a particular type of encryption. Decisions about how to implement encryption 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 electronic communications and information. This aligns with the approach taken in other similar circumstances, including section 187BA of the *Telecommunications (Interception and Access) Act 1979* (Cth).

92. The Department must also protect information from unauthorised interference or unauthorised access (subclause 25(b)).

93. As part of current operations, the Department has implemented a number of measures that will satisfy the requirements in the IVS Bill and protects the security of identification information and the identity verification services. For example, entry into the system (built to PROTECTED classification) is controlled through a Secure Internet Gateway that authorises traffic from approved IP sources and inspects all data traffic to block threats based on real-time intelligence. The internal system elements are segregated and communication between environments is prohibited.

94. Furthermore, all communications and databases are encrypted using the Australian Signals Directorate's military grade approved cryptographic algorithms, and access to the system is strictly controlled, with all users and administrators required to have individual accounts that undergo strong authentication protocols. There is also automated real-time security scanning for vulnerabilities to continuously mitigate any emerging threats.

95. In addition to the security requirements in the IVS Bill, additional obligations can be established through access policies. Clause 14 provides for access policies which will set out additional requirements for entities when requesting identity verification services. Access policies must be complied with by parities to participation agreements (subclause 14(a)).

96. Access policies are another means by which the Department can protect the security of the facilities, ensure they are only used for appropriate purposes, and protect the privacy of individuals. For example,

the Department may use access policies to require entities to comply with new security standards or best practice guidance.

Security and data breach notification requirements

97. The IVS Bill includes reporting requirements for security breaches and data breaches to ensure appropriate action can be taken to prevent the exposure of personal information and remediate any deficiencies in the system.

98. Entities that are a party to a participation agreement will be required to notify the Department of any breaches of security relating to the services (subclause 9(2)(e)). This will enable the Department to take a holistic approach and take steps to prevent identification information from being compromised, and work with government and industry to prevent any such breaches from occurring in the future.

99. Subclause 9(2)(f) requires the Department to inform the Information Commissioner if a security breach amounts to a data breach that is reasonably likely to result in serious harm to individuals 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 Part IIIC of the Privacy Act. This reporting obligation does not impact the application of the Notifiable Data Breach Scheme in relation to those entities that are subject to the Privacy Act, and state and territory notification requirements, for example, the Victorian Protective Data Security Framework and Standards.

100. Similarly, the IVS Bill provides reporting requirements for the NDLFRS. Subclause 13(3)(c) requires state and territory government authorities that are a party to the NDLFRS hosting agreement to inform the Department and individuals if their identification information in the NDLFRS is subject to a data breach which is reasonably likely to result in serious harm to the individual.

101. These notification requirements are intended to minimise harm in the event of a data breach. It provides individuals and the Department with visibility of the nature of personal information involved in a breach, the scope of the breach, and the particular risks of harm flowing from the breach. This will enable the Department to take appropriate action including by reporting the data breach to the Information Commissioner in accordance with the Notifiable Data Breach Scheme.

102. Subclause 13(4)(b) requires the Department to inform state and territory government authorities of any data breaches in the NDLFRS which relates to their jurisdiction's information. This ensures state and 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. It may also enable jurisdictions to review their own security practices and report any breaches to the relevant state or territory government authority.

103. Subclause 13(4)(c) also requires the Department to inform the Information Commissioner if the data breach is reasonably likely to result in serious harm. This aligns with the notification requirements at subclause 9(2)(f) and ensures that the Information Commissioner can take appropriate action in relation to serious data breaches involving the identity verification services and the NDLFRS.

Penalties for non-compliance

104. Subclause 12(c) enables the Department to suspend or terminate an entity's ability to request identity verification services if they do not comply with the privacy safeguards and obligations in the participation agreement, including those in relation to consent and reporting of security breaches, or additional obligations set out in access policies.

105. The potential impact of a suspension or termination may be severe and is expected to act as a deterrent against non-compliance. Suspension or termination would have significant consequences, including financial and reputational damage, given that the use of the identity verification services is critical to industry and providing services to customers.

106. In practice, the annual audit (subclause 12(a)) and compliance reporting requirements (subclause 12(b)) may identify breaches and trigger the Department to consider whether an entity's ability to request identity verification services should be suspended or terminated. The annual audit and compliance reporting are discussed below.

Oversight and transparency

107. The IVS Bill provides extensive oversight and transparency arrangements to ensure the identity verification services are used appropriately and as intended.

Annual auditing and compliance requirements

108. Entities that are a party to the participation agreement must undertake annual audits of compliance with the agreement, including the privacy safeguards and obligations, and report annually to the Department (subclause 12(a) and (b)). Similarly, subclause 13(3)(e) requires state and territory authorities that contribute data to the NDLFRS to report annually to the Department on their compliance with the NDLFRS hosting agreement.

109. These requirements allow the Department to monitor compliance with a participation agreement and NDLFRS hosting agreement, and supports with the development of the annual report (clause 41).

110. They will also support the ongoing administration of the identity verification services. The information obtained through these processes will allow the Department to monitor whether participation agreements and access policies (required under clause 14) remain appropriate and will also inform other oversight processes, including the Information Commissioner's annual assessment (clause 40) and the review of the IVS Bill and identity verification services (clause 43).

Annual assessment by the Information Commissioner

111. The Information Commissioner will conduct an annual assessment on the operation and management of the approved identity verification service facilities (clause 40) – the DVS Hub, Face Matching Service Hub and NDLFRS. As discussed above, these facilities are the technical components that enable the Department to electronically communicate requests between government data holding agencies and those entities using the identity verification services.

112. The policy intent of this important assurance mechanism is to enable the Office of the Australian Information Commissioner (OAIC) to conduct risk-based, forward looking assessments focussed on identifying relevant privacy risks in the system. It is proposed that the OAIC will then be able to make best practice recommendations and suggestions to the Department in relation to the operation of the privacy aspects of the system. While the nature of the assessments will likely change each year, the intended outcome is that the identity verification services will operate in accordance with best practice privacy standards.

113. As an independent agency, the OAIC will determine the scope of the assessments following consultation with the Department. However, potential examples for matters to be considered as part of the annual assessment include, but is not limited to:

- 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.

114. The Information Commissioner must provide the Secretary of the Department with a written report on the assessment. Both the assessment and reporting aspects of this assurance function will be required within 6 months of the end of each financial year ending after the commencement of the IVS Bill.

115. To facilitate the annual assessment, the Secretary must ensure there is an appropriate arrangement in place to ensure the Information Commissioner has access to the information needed to conduct the assessments.

Annual report

116. The IVS Bill requires the Secretary to give the Minister a report each financial year in relation to the operation and use of the identity verification services (clause 41).

117. The annual report is intended to provide public transparency and support Parliamentary scrutiny of the operation of the identity verification services and IVS Bill. In particular, it will provide public visibility of the use of the identity verification services and compliance with the IVS Bill, including the privacy safeguards and security arrangements.

118. Key elements of the annual report include:

- statistics relating to all requests in the financial year for a 1:1 matching service (the DVS and FVS)
- the number of times 1:many matching (the FIS) was used in a financial 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
- information about security incidents and data breaches in connection with the approved identity verification facilities and actions taken in response to any incidents, and
- information about action taken to suspend or terminate access to the identity verification services.

119. The Secretary must provide the annual report to the Minister within 6 months of the end of the financial year. The Minister must table a copy of the annual report in each House of Parliament within 15 days of receipt.

Review of the operations of the Act

120. Within two years of the commencement of the IVS Bill, the Minister must start a statutory review of the operation of the Act and the provision of the identity verification services (clause 43). The two-year period will allow sufficient time for the identity verification services to operate which will enable a more meaningful review to be conducted.

121. This formal review will provide an opportunity to ensure that the IVS Bill (once enacted) is operating as intended and the privacy and security safeguards remain appropriate. The outcome of this review may require certain aspects of the legislation to be reconsidered to ensure the privacy of Australians continues to be protected to the highest standard.

122. The Minister must table a report with the outcome of the review in each House of Parliament. This will provide public transparency and continued Parliamentary scrutiny of the operation of the identity verification services.

Transparency of governance documents

123. The IVS Bill requires that a participation agreement, the NDLFRS hosting agreement and other relevant documents are published on the Department's website, as well as any documents varying, terminating or revoking any of these documents (subclause 39(1)). 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.

124. This strikes an appropriate balance by enabling key information about the development, operation and maintenance of the identity verification services to be made publicly available while protecting privacy and preventing any risk of harm to the security of identification information and systems, individuals, or Australia's national security.

Outline of the Consequential Amendments Bill

125. 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.

126. As the NDLFRS is currently not operational, an Australian Passport is the only government issued identity credential that enables biometric verification. As discussed above, biometric verification is a highly secure way of verifying identity and is currently required to create a 'strong' myGovID.

127. The Consequential Amendments Bill amends the *Australian Passports Act 2005* (Passports Act) to allow for automated disclosures of personal information to a specified person via the DVS and FVS. This will comprehensively authorise the operation of the DVS and FVS in relation to Australian travel documents regulated by the Passports Act.

128. This aligns with the current operational needs of the Department of Foreign Affairs and Trade (DFAT) 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. The amendments do not allow for the automated disclosure of personal information to the FIS.

129. As reflected in the note at the end of current section 46 of the Passports Act, information disclosure authorised by the amendments 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 the amendments.

130. These and other privacy safeguards, accountability and transparency measures in the IVS Bill should provide the Australian community with confidence that their personal information on an Australian Passport is protected.

Conclusion

131. The IVS Bill and Consequential Amendments Bill will establish strong and secure identity verification to enhance the privacy of Australians. They support the efficient and secure operation of the identity verification services, and meets public expectations that the services have extensive privacy safeguards and effective oversight and transparency requirements. The legislation will enable Australians to conveniently and securely engage with the digital economy and access critical services while minimising the risk of identity fraud and theft.