MEMORANDUM OF UNDERSTANDING

Department of Home Affairs

and

Department of Veterans' Affairs

FOR PARTICIPATION AS A USER IN THE

NATIONAL DOCUMENT VERIFICATION SERVICE

Contents

Part A – PARTIES, PURPOSE AND BACKGROUND

1 Parties and Purpose

1.1 This Memorandum of Understanding (MOU) is entered into between the Commonwealth of Australia represented by the Department (Home Affairs) and the Department of Veterans' Affairs] (the Organisation) (herein jointly referred to as of Home Affairs the 'Parties') for the national Document Verification Service (DVS).

1.2 There is no intention for this MOU to create a legal relationship between the Parties; it does not create legally binding obligations on the Parties. It clarifies the relationship between Home Affairs and the Organisation, as a DVS User, and provides a level of detail about various roles, responsibilities and requirements, which operate to ensure the integrity of the DVS.

1.3 This agreement comprises of the following parts:

(a) this MOU;

(b) Schedule 1 (Services Schedule);

(c) Schedule 2 (Contact Information);

(d) Schedule 3 (Interpretation);

(e) Schedule 4 (MOU Variation Template);

(f) Addendum 1 (Compliance Statement); and

(g) Addendum 2 (Current Users).

1.4 This MOU supersedes any prior communications, arrangements or understandings between Home Affairs and the Organisation on the subject matter of this MOU and its schedules, including any previous Memoranda of Understanding.

2 Background

Implementing the DVS

2.1 The National Identity Security Strategy (NISS) was developed in 2007 after the Council of Australian Governments (COAG) agreed that the preservation and protection of a person's identity is a key concern and a right of all Australians. Since then, the NISS has substantially advanced the cause of identity security. Key achievements include the establishment of the DVS and the development of several national standards related to identity management.

2.2 COAG agreed to a revised strategy in 2012 to revitalise the national identity security agenda following a review of the NISS. The revised strategy has been developed to ensure Australia's approach to identity is ready to meet the opportunities and challenges presented by the digital economy and respond to the rapidly evolving nature of identity crime in Australia.

2.3 The DVS enables Users to enhance their overall risk management approach and have greater confidence in the integrity of Identifying Information, which may be provided to them by individuals as evidence of their identity when registering or enrolling for a benefit or service or applying for additional identification documentation or credentials. Examples of types of Identifying Information that can be verified include passports issued by the Australian Passports Office and citizenship certificates or visas issued by the Commonwealth Department of Immigration and Border Protection.

The DVS Hub

2.4 This DVS Hub acts as a secure conduit for Users to confirm with Issuers that Identifying Information is valid and has not been cancelled, superseded, reported lost or stolen. The DVS does not retrieve or store any personal information held by the Issuer.

The DVS ICT Operations Manager

2.5 The DVS ICT Operations Manager maintains all applications, resources and systems support for the DVS Hub so that the DVS Hub and its links or interfaces with Users and Issuers operate with a high level of speed, reliability, responsiveness and accuracy.

2.6 The DVS ICT Operations Manager also provides technical assistance and support to Users and Issuers.

Connection to the DVS

2.7 The Organisation may access the DVS through a:

(a) Standard Connection;

(b) Gateway Service Provider;

(c) Whole of Government Connection; or

(d) by other means as agreed with Home Affairs.

Part B – TERM AND GOVERNANCE

3 Term, Expiry and Termination

3.1 This MOU will commence immediately after both Parties have signed it and will continue unless terminated in accordance with Item 22.

4 Governance

4.1 The National Identity Security Coordination Group (NISCG) is the central jurisdictional consultative forum responsible for the implementation of the NISS, and is the peak decision-making body of the DVS.

4.2 The National DVS Advisory Board reports to the NISCG and is responsible for considering significant aspects of DVS design and operation.

4.3 The DVS Manager is responsible for operational management and policy implementation and reports to the National DVS Advisory Board and NISCG.

4.4 The Business and Technical Working Group (BTWG) advises and reports to the National DVS Advisory Board (and NISCG if required) on business and technical matters.

4.5 The DVS Program Commonwealth Steering Committee oversees and monitors progress on the DVS program objectives and resolving operational and policy issues.

4.6 Each Party appoints the:

(a) Primary Contact Officer; and

(b) contacts in the Contact Protocols

as specified for that Party in **Schedule 2 – Contact Information** or as otherwise notified in writing by a Party to the other Party from time to time.

Part C – ROLES AND RESPONSIBILITIES

5 Responsibilities of Home Affairs

5.1 Home Affairs acknowledges that its role in the DVS includes:

(a) working with Issuers and Users to maintain the integrity of the DVS through the implementation of appropriate measures;

(b) working closely with the National DVS Advisory Board in reaching decisions about the DVS;

(c) acting on behalf of Issuers and Users in regard to the DVS;

(d) assisting Issuers with Threat and Risk Assessments prior to connecting to the DVS Hub;

(e) being a DVS User;

(f) maintaining a suite of DVS Supporting Material;

(g) being the central point of contact for any public enquiries about the DVS and coordinating any necessary public statements;

(h) conducting any due diligence processes for commercial organisations applying to become a Gateway Service Provider required by the DVS Access Policy and Guidelines;

(i) approving Gateway Service Providers and government users; and

(j) acting as secretariat to the National DVS Advisory Board, DVS Program Commonwealth Steering Committee and BTWG.

5.2 Home Affairs agrees to:

(a) work with the Organisation to maintain the integrity of the DVS through the implementation of appropriate security and privacy safeguards; and

(b) provide the Organisation with access to DVS Supporting Material as updated from time to time.

6 Responsibilities of the Organisation

General

6.1 The Organisation acknowledges that:

(a) the relationship between the Parties operates in a framework where there will be iterative implementation and development, changing technology and emerging policy issues that could require changes to the relationship and this MOU; and

(b) participating in the DVS requires full cooperation and consultation with all Parties.

7 Privacy

7.1 The Organisation acknowledges that while technical aspects of the DVS have been designed in a way that are respectful of privacy, it is important to ensure that measures are in place to maintain the integrity of the DVS and to protect privacy.

7.2 The Organisation agrees that, at a minimum, it will implement measures to:

(a) handle complaints;

(b) respond to requests for;

i. access to information; and

ii. reviews of decisions on identity in accordance with the Organisation's own procedures and relevant privacy requirements, and

(c) comply with all requirements contained in Commonwealth and State/Territory privacy legislation relevant to its jurisdiction, including, at all times Australian Privacy Principle 9.2.

8 Consent

8.1 As a User, the Organisation agrees to obtain consent from individuals to match the Identifying Information contained on evidence of identity documents and informing individuals:

(a) that the details are being collected to confirm the integrity of the Identifying Information;

(b) the Identifying Information will be checked with the Issuer or Official Record Holder; and

(c) of any legal authority under which the details of the Identifying Information are being collected.

8.2 The Organisation understands that the measures contained in this MOU and the DVS Supporting Material do not replace other requirements, such as those contained in privacy legislation relevant to its jurisdiction.

9 Technical Requirements and Information Security

9.1 The Organisation agrees that it is responsible for its own technical links and interface with the DVS Hub and any costs associated with the provision of management information on its performance or the performance of the DVS.

9.2 The Organisation acknowledges the importance of maintaining high levels of security for the DVS and the need to ensure appropriate measures are in place to reduce or minimise any security risk or threat to the DVS, and to ensure that privacy is protected.

9.3 The Organisation agrees that, at a minimum, it will implement measures ensuring it:

(a) complies with all security procedures advised to it in relation to the DVS and will take all reasonable action to protect and maintain the security of the DVS and its access to and use of it, including, without limitation, maintaining the security of all tokens, access codes, encryption keys and other information relating to access, authentication or security relating to the DVS;

(b) takes all reasonable action to prevent and detect unauthorised use of the DVS;

(c) immediately notifies Home Affairs of unauthorised use, security breaches, suspected security vulnerabilities, faults and errors or problems with the DVS or any Information Match Result;

(d) complies with the requirements set out in the Protective Security and Information Security policies and procedures applicable to its jurisdiction; and

(e) any other responsibilities outlined in Schedule 1.

10 Additional Protocols

10.1 The Organisation acknowledges the importance of implementing additional protocols to maintain and enhance the integrity of the DVS.

10.2 The Organisation agrees that:

(a) the DVS is designed to assist but not replace existing Identity Proofing processes and procedures;

(b) a positive or negative response received through the DVS will not be used as the sole basis for a decision to enrol or not enrol an individual for benefits or services, or to issue or not issue Identifying Information to an individual; and

(c) handling complaints, responding to access for information requests and reviews of decisions are to be carried out by the Organisation in accordance with its own procedures.

11 Management and Reporting

11.1 Each Party agrees to provide any other information relating to this MOU to the other Party when reasonably requested by the other Party to do so (for example, to assist in satisfying a Party's service management, reporting or accountability requirements), within the timeframe reasonably required.

Part D – SERVICE REQUIREMENTS

12 ICT Arrangements and Maintenance

12.1 In order to facilitate the provision of the Services, the Parties will work together to ensure that their respective information technology arrangements facilitate the effective and efficient provision of the Services.

12.2 For the purposes of this MOU, the Organisation will only be responsible for the maintenance of its ICT components that contribute to its participation in the DVS.

12.3 The Organisation agrees with any other requirements set out in Schedule 1.

13 Compliance

13.1 The Organisation acknowledges the importance of ensuring compliance with DVS requirements to maintain and enhance the integrity of the DVS. To this end, the Organisation agrees to submit a compliance statement to Home Affairs on the 31st January each year or at the request of Home Affairs for consideration by the National DVS Advisory Board.

13.2 The Organisation agrees that, at a minimum, its compliance statement will contain information that supports its claim that its use of the DVS is in accordance with this MOU and that it has implemented appropriate technical, privacy and security safeguards. A preferred form of compliance statement has been made available to the Organisation at Addendum 1.

13.3 The Organisation agrees to provide recommendations that may be made to it in relation to its use of the DVS to the National DVS Advisory Board as information becomes available. This information may come from reports to the Organisation from areas such as:

(a) audits of the Office of the Privacy Commissioner;

(b) review bodies of State/Territories; and

(c) other audits or reviews.

Part E - ASSETS, DATA AND INFORMATION MANAGEMENT

14 Assets

14.1 As between the Parties, all infrastructure, equipment, hardware and other assets used by the Organisation in its participation in the Services are managed by the Organisation.

15 Data

15.1 All data and information provided by Home Affairs to the Organisation in relation to the Services, whether of a corporate, operational or program delivery nature, will be owned by Home Affairs.

16 Risk Planning and Issue Management

16.1 During the term of this MOU, each Party will keep the other Party informed of risks and issues relating to the performance of the Services that come to its attention using mechanisms detailed in this MOU.

Part F – MISCELLANEOUS MATTERS

17 Subcontracting and Service Providers

17.1 The Parties acknowledge and agree that either Party may outsource or subcontract any aspect of the Services to one or more external service providers.

17.2 Where requested, each Party agrees to:

(a) promptly provide all reasonable assistance to enable the other party to comply with its obligations under its contracts with its external service providers; and

(b) cooperate with the party's external service providers as reasonably required to enable the provision of the Services.

18 'Best Efforts'

18.1 The DVS relies on the cooperation and best efforts of all participating Organisations. To this end, both Parties agree not to hold each other partially or wholly liable for any act or omission, system fault or error.

19 Intervening Event

19.1 Where an event occurs which is out of that Party's control, the Party will be excused from fulfilling its responsibilities under this MOU. This includes, but is not limited to, force majeure, natural disasters, acts of war, riots and strikes.

19.2 Without limiting Item 19.1 the Organisation will be excused from performing its responsibilities under this MOU to the extent that it is prevented from doing so by:

(a) a Government policy decision;

(b) an emergency event, as described in Item 19.1 of this MOU, that requires a diversion of the Organisation's resources, in a way that materially affects the Organisation's ability to perform the Services in accordance with Schedule 1; or

(c) a default of one of the Organisation's external service providers, provided that the Organisation exercises all reasonable measures to mitigate the effect of that default.

19.3 Where circumstances described in Item 19.1 or 19.2 arise, the affected Party must give notice to the other Party as soon as possible, and the Parties agree to negotiate in good faith to minimise the impact of any delay on the Services.

20 Disclosure

20.1 Except where disclosure is required by law or is otherwise in accordance with Commonwealth, State or Territory policy, both Parties agree that they will not, without the prior written approval of the other Party, disclose to any third person any MOU material which is confidential to the other Party.

21 Additional Matters

21.1 The Organisation acknowledges that the DVS is offered 'as is and as available' and agrees to implement alternative identity verification processes in the event that the DVS is unavailable or is not fit for purpose.

21.2 Each Party will comply with relevant Work Health and Safety Laws, and will undertake its obligations under this MOU and all schedules in such a way that ensures the health and safety of workers and third parties.

21.3 Each Party will comply with all Commonwealth and State/Territory laws and guidelines on human rights and equal opportunity law relevant to its jurisdiction. Each Party will undertake its obligations under this MOU and all schedules in such a way that ensures compliance with those laws and/or guidelines.

Part G – TERMINATION, VARIATION, SUSPENSION AND DISPUTES

22 Termination

22.1 Either Party can terminate this MOU by giving 3 months written notice to the other (or a different notice period agreed by both Parties).

22.2 Termination costs, if any, are to be determined as agreed by the Parties at the time of termination. However, each Party is to:

(a) take all reasonable steps to mitigate the impact of the cessation of those activities; and

(b) discuss and agree, in good faith, arrangements applicable to that cessation including (where relevant) a fair and reasonable adjustment in amounts payable to the Party ceasing to carry out those activities having regard to the proportion of those activities carried out prior to termination, and to any activity-related costs incurred prior to the termination or incidental to an orderly termination.

23 Variation

23.1 The Parties agree from time to time each party may perform additional Services under the terms of this MOU by amending this MOU or its schedules or by executing the Variation at Schedule 4. Generally, the Parties anticipate that the amendments may address:

(a) additional Services to be provided by the Organisation and/or Home Affairs and any fees payable for those Services; or

(b) the role and responsibilities of either Party;

(c) Addition or removal of Users party to this MOU (these will be recorded at Addendum 2).

24 Suspension

24.1 Home Affairs, in consultation with the National DVS Advisory Board, may suspend the Organisation from participating in the DVS and take all necessary steps to give effect to that suspension if Home Affairs considers on reasonable grounds that the Organisation:

(a) has or may adversely affect the security, privacy, reputation, stability or integrity of the DVS;

(b) has or may contravene any of the laws of Australia;

(c) has or may use the DVS contrary to the terms of this MOU;

(d) has failed to make payments of fees within the allocated period; or

(e) has breached other terms of this MOU.

24.2 A suspension under Item 24.1 may be temporary or indefinite and does not terminate this MOU.

24.3 Home Affairs must, if practical, provide the Organisation with reasonable advance notice of its intention to suspend the Organisation's participation in the DVS and provide the Organisation with an opportunity to cease, remedy or ameliorate any activity or circumstance which Home Affairs considers may justify the Organisation's suspension from the DVS under Item 24.1.

24.4 Should Home Affairs suspend the Organisation's participation in the DVS, Home Affairs must provide the Organisation with a written notice that it has been suspended and the reason for suspension. During the period of any suspension Home Affairs and the Organisation must work cooperatively to cease, remedy or ameliorate any activity or circumstances which lead to the suspension being imposed or continued.

24.5 The Organisation has the opportunity to appeal the decision of Home Affairs to the Deputy Secretary, National Security & Emergency Management, Department of Home Affairs (Deputy Secretary) within 14 days of a notice of suspension being issued.

25 Dispute Resolution

25.1 The Parties agree to consult fully with each other, other Issuers and Users, the DVS ICT Operations Manager and any other affected party to resolve any issue in connection with the DVS or this MOU. In the event that issues are not resolved within a reasonable period of time either Party may refer to the First Assistant Secretary, National Security Division for resolution.

Part H – SIGNATORIES

26.1 This MOU was entered into by the Parties on Wednesday 21 March 2018.
13 April

Signed for, and on behalf of, the Commonwealth of Australia by Andrew Rice, Assistant Secretary, Identity and Biometrics Division, Department of Home Affairs, in the presence of:

s. 22(1)(a)(ii)

witness name

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

signature of witness

Signed by s. 22(1)(a)(ii) Assistant Secretary, VCR Implementation, Department of Veterans' Affairs], in the presence of:

s. 22(1)(a)(ii)

witness name

s. 22(1)(a)(ii)

signature of representative

s. 22(1)(a)(ii)

signature of witness

Schedule 1 – Services Schedule

1. Roles and Responsibilities

1.1 The Organisation agrees that, at a minimum, it will:

(a) continue to operate, develop, test, implement and manage any Interface with the DVS Hub in accordance with technical, privacy and security requirements contained in this MOU and the DVS Supporting Material;

(b) promptly comply with all reasonable directions from the DVS ICT Operations Manager pertaining to access and use of the DVS Hub;

(c) nominate an individual to act as the point of contact with the DVS ICT Operations Manager on technical issues; report privacy and security breaches to Home Affairs, the DVS ICT Operations Manager or any other relevant entity as appropriate;

(d) report any significant fault in terms of accessing the DVS Hub and/or an Issuers Service to the DVS ICT Operations Manager immediately so that fault may be rectified;

(e) cooperate with the DVS ICT Operations Manager to rapidly identify the cause of operating problems that reduce the performance of the DVS below the standards stated in this Schedule 1;

(f) ensure that its personnel are made aware of privacy and security obligations prior to using the DVS;

(g) handle suspected or actual breaches of privacy or security involving the DVS in accordance with the DVS Supporting Material;

(h) retain information in connection with the use of the DVS for audit and compliance purposes and to fulfil privacy and record keeping obligations as required in its jurisdiction; and

(i) participate in at least one disaster recovery exercise per year.

2. Information Security

2.1 The Organisation agrees that:

(a) its use of DVS technical components, including access to the DVS Hub, will be restricted to authorised personnel and controlled through secure logons and passwords;

(b) its interfaces do not allow for DVS Hub messages to be retrieved or reviewed outside of the DVS;

(c) its use of DVS technical components, including access to the DVS, does not permit unauthorised access to technical components, systems or software;

(d) its use of DVS technical components, including access to the DVS, does not disable, damage or disrupt technical components, systems or software;

(e) its staff receive regular training and awareness programs on social engineering risks and its mitigations; and

(f) a regular review of processes is conducted to ensure appropriate measures are in place to reduce or minimise any risk or threat to the DVS.

3. Incident Management

3.1 The components of the DVS Support Services are:

(a) Incident Impact, Urgency and Priority Levels

i. The DVS ICT Operations Manager is responsible for ensuring that Service Incident resolution conforms to the impact, urgency and priority levels stated below:

Level	Considerations
Impact	Considers the business impact (service Degradation) upon: • DVS Users / GSPs • DVS Issuers • DVS Hub
Urgency	The speed that Incidents are expected to be resolved: • Critical: o Any Incident causing an Outage of the DVS Hub. • High: o An Incident preventing a DVS User from accessing the DVS Hub or processing transactions. o The system is producing multiple Hub 'S' results to one or more users. • Medium: o An Incident has occurred that has minor impact on operations during Core Support Hours. Transaction processing continues, e.g. One document type is returning intermittent S results • Low: o An Incident where a work-around is available and impact is mostly transparent to all DVS Users or impacts only a single DVS User.
Priority	In accordance with ITIL principles, Service Levels are based on the priority of the Incident as derived from Impact and Urgency metrics. • A single Priority Level should be assigned to each Incident at any point in time, derived from the following scale: o P1 – Critical (highest priority) o P2 – High o P3 – Medium o P4 – Low

Priority Levels derived from Impact and Urgency Levels

PRIORITY (To Be Assigned)		**URGENCY**			
		Critical	*High*	*Medium*	*Low*
IMPACT	*DVS Hub*	P1	P1	P2	P3
	DVS Issuers & GSPs	P1	P1	P2	P3
	DVS Users	P2	P2	P3	P4

(b) Response and Resolution Times

ii. DVS ICT Operations Manager must conform to the priorities, response and resolution times.

iii. DVS Support must confirm the priority level at the time the Incident is logged, in consultation with the incident originator.

iv. All Priority 1 Incidents must be logged by DVS participants as 'critical' via the DVS Incident Portal.

v. If a Priority 1 or Priority 2 Incident is logged during Core Support Hours specified in Table 10, the Incident management action will continue out of Core Support Hours until the Incident is resolved.

vi. Priority 3 and 4 Incidents are resolved and worked during Core Support Hours. Where Priority 3 and 4 Incidents occur out of Core Support Hours, the Resolution Time (including Response Time) will be paused during the out of Core Support Hours period.

vii. DVS Support must broadcast a status update to relevant DVS participants throughout the resolution period.

viii. Resolution Time includes the allocation for Response Time.

Response and Resolution Times

Priority	**Response Time**	**Resolution Time** (includes Response Time)	**Update Time**
P1	15 minutes	4 hours	Every 30 minutes
P2	30 minutes	8 hours	Every 60 minutes
P3	2 business hours	18 business hours	Every 9 business hours
P4	9 business hours	72 business hours	As agreed

DVS Support Hours of Business

Core Support Hours	Monday to Friday (5 days) 8:30am to 5:30pm (AEST / AEDT) excluding National and ACT Public Holidays
Out of Hours Support	Monday to Sunday (7 days) All hours outside Core Support Hours including National and ACT Public Holidays

i. Incidents can be logged with DVS Support during Core Support Hours and Out of Hours via the DVS Incident Portal

DVS Incident Portal	s. 47E(d)

4. Service Fees

4.1 The preferred position on costs associated with the use of the DVS is for Issuers to not charge government users for access to its verification services.

4.2 Home Affairs reserves the right to introduce User charges for access to the DVS and the timing for introducing charges will be subject to agreement with the Organisation.

4.3 The Organisation will pay any fees associated with its connection to the DVS, as agreed with Home Affairs. A Standard Connection to the DVS is s. 47D GST Exclusive) which is payable on presentation of an invoice by Home Affairs.

4.4 If an Organisation connects to the DVS via a Gateway Service Provider the Organisation will not be liable for the Standard Connection fee identified in clause 4.3.

4.5 If an Organisation connects to the DVS but does not use a Standard Connection, Gateway Service Provider or existing Whole of Government connection, Home Affairs will assess the Organisation's liability for fees associated with the connection.

4.6 The Organisation will pay any fees associated with a variation to this MOU in the allocated timeframe, as agreed with Home Affairs.

4.7 The Organisation will make all reasonable efforts to comply with any electronic invoicing requirements notified by Home Affairs.

5. Communications

5.1 All communications required or contemplated by this MOU from one Party to the other must be in writing (including email) and must be sent to, or copied to the Primary Contact Officer for the receiving Party. This Item does not apply to general operational correspondence that is not specifically required or contemplated by this MOU and does not apply to Incident management reporting where the Contact Protocols apply.

Schedule 2 – Contact Information

General Contact Details:

Department of Veterans' Affairs

Contact information:
Department of Veterans' Affairs
s. 22(1)(a)(ii)
Canberra ACT 2600

Primary Contact Officer:
s. 22(1)(a)(ii)
Director
VCR Implementation
Ph: s. 22(1)(a)(ii)
s. 22(1)(a)(ii)@dva.gov.au

Senior Representative:
s. 22(1)(a)(ii)
Director
VCR Implementation
Ph: s. 22(1)(a)(ii)
s. 22(1)(a)(ii)@dva.gov.au]

Senior Executive Contact:
Matt McKeon
Assistant Secretary
VCR Implementation
Ph: s. 22(1)(a)(ii)
s. 22(1)(a)(ii)@dva.gov.au

Department of Home Affairs

Contact information:
Department of Home Affairs
3-5 National Circuit
Barton ACT 2600
DVS.manager@homeaffairs.gov.au

Primary Contact Officer:
s. 22(1)(a)(ii)
Project Officer
Identity Security Branch
Ph s. 22(1)(a)(ii)
s. 22(1)(a)(ii)@homeaffairs.gov.au

Senior Representative:
s. 22(1)(a)(ii)
Director
Identity Security Branch
s. 22(1)(a)(ii)@homeaffairs.gov.au

Senior Executive Contact:
Andrew Rice
Assistant Secretary
Identity Security Branch
Phs. 22(1)(a)(ii)
s. 22(1)(a)(ii)@homeaffairs.gov.au

Contact Protocols:

	The Organisation	Home Affairs
GENERAL INCIDENTS During business hours	MyService support 8:30am – 5:00pm 02 6289 6015 Email: myservicesupport@dva,gov.au	DVS Manager 8:30am – 5:00pm Ph: 02 6141 2723 Email: s. 22(1)(a)(ii)@homeaffairs.gov.au
CRITICAL INCIDENTS **During Business Hours**	**Primary Point of Contact** myservicesupport@dva,gov.au **Escalations** Director DCE s. 22(1)(a)(ii) @dva.gov.au	**Primary Point of Contact** s. 47E(d) **Escalations** DVS Manager s. 22(1)(a)(ii) Ph: s. 22(1)(a)(ii) Email: s. 22(1)(a)(ii)@homeaffairs.gov.au s. 22(1)(a)(ii)
CRITICAL INCIDENTS **Outside of Business Hours**	**Primary Point of Contact** myservicesupport@dva,gov.au **Escalations** Director DCE s. 22(1)(a)(ii) @dva.gov.au	**Primary Point of Contact** https://servicedesk.oakton.com.au/ **Escalations** DVS Manager s. 22(1)(a)(ii) Ph: s. 22(1)(a)(ii) Email: s. 22(1)(a)(ii)@homeaffairs.gov.au 0429 054 077
CHANGE REQUESTS	**Primary Point of Contact** Director DCE s. 22(1)(a)(ii) @dva.gov.au	**Primary Point of Contact** DVS Manager s. 22(1)(a)(ii) Ph: s. 22(1)(a)(ii) Email: s. 22(1)(a)(ii)@homeaffairs.gov.au s. 22(1)(a)(ii)

Note: A Party can update its Contact Protocol details by written notice to the other Party under Item 4.6 of this MOU.

Schedule 3 - Interpretation

Definitions

In this MOU, the following capitalised terms have the meaning given below unless the context otherwise requires:

Australian Privacy Principle 9.2 means the subclause in Schedule 1 of the *Privacy Act 1988* related to the use or disclosure of government related identifiers.

Home Affairs has the meaning provided in Item 1.1.

AEDT means Australian Eastern Daylight Savings Time.

AEST means Australian Eastern Standard Time.

Business and Technical Working Group (BTWG) means the group responsible for making technical decisions relating to the DVS and its Issuing Agencies.

Business Day means a day Monday to Friday that is not a public holiday in the Australian Capital Territory, but does not include any days between 26 December and 1 January (inclusive) in any year.

Compliance Statement Template means the template provided at **Addendum 1** for assessing the Organisation's compliance with the terms of the MOU.

Contact Protocols has the meaning provided in **Schedule 2 – Contact Information**.

Core Support Hours has the meaning provided in clause Item 3.1 of **Schedule 1 – Services Schedule.**

Council of Australian Governments (COAG) means the group responsible for approving the National Identity Security Strategy.

Degradation means that the speed of Issuer transaction response for any document type is higher than an average of 5 seconds.

DVS has the meaning provided in Item 1.1.

DVS Access Policy and Guidelines means the policy under which eligibility of new DVS commercial users is assessed.

DVS Hub means the components of DVS infrastructure that connect Issuers and Users and allow for DVS match requests and responses to be securely routed between them.

DVS ICT Operations Manager means the entity engaged by the Home Affairs to operate the DVS Hub, as described in Items 2.5 and 2.6.

DVS Incident Portal means the online reporting tool for raising DVS incidents.

DVS Manager means the entity engaged in Home Affairs to manage the DVS.

DVS Support means the DVS Hub ICT Operations Manager dedicated Support team.

DVS Support Services means the services provided by DVS Support

DVS Supporting Material means information about governance and operational arrangements, technical requirements, security, privacy and support. This information is available from Home Affairs and is made available to all DVS Issuer and Users.

Gateway Service Provider means a third party entity, approved by Home Affairs, to provide Users with access, or access services, to the DVS.

Identifying Information means information that may function for identifying purposes such as may be found in passports, Medicare cards, visas, citizenship certificates, registration by descent certificates, ImmiCards, birth, marriage and change of name certificates and drivers' licences.

Identity Proofing or **ID Proofing** means part of the enrolment process by which the Registration Authority captures and verifies sufficient information to identify a person to a specified or understood level of assurance.

Incident means any incident, occurrence, fact or circumstance that does or reasonably might:

(a) causes a disruption to a Service; or
(b) affects the quality or timeliness of a Service as required to be provided pursuant to this MOU.

Information Match Request means an electronic request to the DVS by a User (required to be submitted in a structured electronic format advised by Home Affairs) to be provided with an Information Match Result in relation to the details of relevant information in Identifying Information.

Information Match Result means, in respect to an Information Match Request, an electronic response indicating that the information provided in the request either matches or does not match the relevant official record data, or that a system error has been encountered in trying to process that request.

Interface means the software and hardware that enables technical connections with the DVS Hub.

Issuer means an organisation that can respond to a DVS match request from a User through the DVS Hub.

Issuer Services means provision of a response to a request from a User to match Identifying Information through the DVS Hub.

National DVS Advisory Board means the Board established as part of the National Identity Security Strategy to consider significant aspects of the operations of the DVS and provide a forum to discuss and resolve governance, operational and technical issues; including dispute resolution. It is accountable to the NISGC.

National Identity Security Coordination Group means the group accountable for work items under the National Identity Security Strategy.

National Identity Security Strategy (NISS) means the Strategy under which the DVS was formed.

Office of the Privacy Commissioner means the Office of the Australian Information Commissioner established by the *Australian Information Commissioner Act 2010* (Cth).

Official Record Holder has the same meaning as **Issuer**.

Organisation has the meaning provided in item 1.1

Outage means an occurrence within the Organisation's ICT environment that results in the partial or complete cessation of the Issuer service.

Parties has the meaning provided in item 1.1

Primary Contact Officer means a person specified such for a party in **Schedule 2- Contact Information** or as otherwise notified by a party to the other party from time to time who has responsibility for day-to-day management of the MOU.

Relevant Work Health and Safety Laws means work health and safety laws in the Commonwealth, and State and Territory laws where applicable and as amended from time to time, including:

Work Health and Safety Act 2011 (Commonwealth); and

Work Health and Safety Regulations 2012 (Commonwealth).

Resolution Time means the time elapsed from initial receipt of the Incident by the DVS Support to resumption of full normal operations because:

(a) the Incident has been resolved;

(b) a workaround has been implemented; or

(c) a plan for resolution has been agreed where the resolution factors are beyond the control of the Service Provider.

Response Time means the time elapsed from initial receipt of the Incident by DVS Support to the time a support person issues a notification to confirm that the Service Provider has commenced a diagnosis of the Incident.

Senior Representative means a person specified such for a party in **Schedule 2 – Contact Information** or as otherwise notified by a party to the other party from time to time who has senior responsibility for the management of this MOU.

Senior Executive Contact means a person specified such for a party in **Schedule 2 – Contact Information** or as otherwise notified by a party to the other party from time to time who is authorised to enter into this MOU and any subsequent MOU Variations.

Services means a service provided under this MOU and includes any Material, goods or other item to be provided or delivered as part of or incidental to that service (which unless otherwise specifically agreed to the contrary in writing by Home Affairs includes provision of all data created in the course of provision of the service.

Service Availability has the meaning provided in clause Item 3.1 of **Schedule 1 – Services Schedule**.

Service Hours represent the minimum hours for which ICT Services are scheduled as available for use. Service Hours are kept free of planned Outages or Degradation of performance or capacity except as per the constraints listed in **Schedule 1 – Services Schedule**.

Service Levels has the meaning provided in Item 3 of Schedule 1 – Services Schedule.

Signatory means the authorised executive who has signed this MOU.

Standard Connection means a direct webservice connection to the DVS, using compatible software, with access to all supported document types.

Term has the meaning provided in Item 3.1.

Threat and Risk Assessments means threat and risk assessments undertaken by an Infosec-Registered Assessor Program (I-RAP) accredited assessor.

User means an organisation that seeks to validate information provided by an individual as evidence of its identity with an Issuer, by request through the DVS Hub.

Variation means any modification to the terms originally agreed and set out in the MOU.

Whole of Government Connection means a connection to the DVS facilitated by a state Government arrangement. The state Government is responsible for all connected users connecting through the Whole of Government arrangement and will ensure each user meets all the requirements of this memorandum of understanding.

Schedule 4 – Variation Template

This form will be used to record amendments to current arrangements, including administrative, financial, technical and/or legislative aspects. Please lodge this form through the relevant Contact Officer.

Variation Request Number	Variation Number [#] of [Year] to the Memorandum of Understanding of [Date MOU signed] between the Department of Home Affairs and Department of Veterans' Affairs
Title	
Date of Request	
Variation Description	In accordance with paragraph 23.1 of the MOU signed on [date MOU signed], the MOU is varied as follows: 1. *[Description of the nature of the request. i.e. additional services to be performed, update to this agreement etc.]* 2. *[Define services to be performed under the variation]* 3. *[Critical information/impacts or additional information]*
Party Initiating Change	**[Organisation]** ☐ **Home Affairs** ☐
Proposed Implementation Date	*[Proposed date for implementation or completion of the services]*

Execution

This Variation No [#] of [Year] to the MOU is entered into by the Parties on the date the Department of Veterans' Affairs authorised delegate agrees by signing below.

Signed for, and on behalf of, the Commonwealth of Australia by Andrew Rice, Assistant Secretary, Identity and Biometrics Division, Department of Home Affairs, in the presence of:

.....
witness name

.....
signature of representative

.....
signature of witness

Signed by [name], [position], [branch], Department of Veterans' Affairs in the presence of:

.....
witness name

.....
signature of representative

.....
signature of witness

Addendum 1 – Compliance Statement Template

Introduction

Each participating DVS Agency has signed a DVS Memorandum of Understanding (MOU) agreeing to abide by its terms and conditions, including that the Agency has implemented appropriate technical, privacy and security safeguards as described in the DVS Supporting Material. As part of measures to maintain and enhance the DVS User and Issuer Agencies are required to submit a Compliance Statement for consideration by Home Affairs and the DVS Advisory Board, at least annually.

The Compliance Statement is a mechanism for the Agency to review and refresh its claim that its use of the DVS is in accordance with the agreed terms.

Preparing the Statement

The essence of the Compliance Statement is that the Agency makes a statement about its performance during the period covered by the Statement on the extent to which it:

> **Complied with the terms of its DVS MOU/Contract and, in particular, has maintained appropriate technical, privacy and security safeguards in accordance with the terms of the DVS MOU/Contract and the related DVS Supporting Material.**

If the Agency did not fully comply with the MOU/Contract, it must advise the remedial action being taken to ensure compliance.

The statement should address the Agency's performance against the agreed terms of the MOU/Contract and the DVS Supporting Material and include information/documentation to the following:

1	**Explain how you would ensure personnel are aware of privacy and security obligations prior to using and whenever using the DVS.** *DVS Best Practise Advice* *The DVS Manager recommends that participating Government agencies should mandate standard privacy and security awareness training with periodic refreshment (every 12-24 months).* *Privacy training should be aligned with the privacy principles (Privacy Act 1988) or a state or territory equivalent.* *Mechanisms should be in place to ensure that any changes to privacy and security policy are communicated to staff.*
2	**Advise how DVS checks would only be undertaken with customer consent.**

	DVS Best Practise Advice *The DVS Manager recommends that all individuals providing personal information to be matched by the DVS:* • *State that they are authorised to provide the personal information to be matched* • *Are informed of the purpose and* • *Consent to this use.* *The DVS Manager provides the following best practise consent statements (inclusive of the checkbox):* *☑I confirm that I am authorised to provide the personal details presented and I consent to my information being checked with the document issuer or official record holder via 3rd party systems for the purpose of confirming my identity.* *Or* *☑I consent to my information being checked with the document issuer or official record holder.* *Where the shorter consent statement is used, other aspects of the consent should be incorporated in supporting material such as Terms and Conditions agreed to by the individual or a published privacy policy.*
3	**How do you ensure personnel are aware that, while using the DVS, they must still comply with other requirements such as those contained in privacy legislation relevant to its jurisdiction?** *DVS Best Practise Advice* *The DVS Manager recommends that participating Government agencies should ensure, where it has provided training on the use of the DVS, this training material explicitly identifies the existence of any additional requirements over and above those contained in the DVS memorandum of understanding.*
4	**How do you ensure personnel are aware that the DVS does not make decisions about identity but provides them support in making those decisions?** *DVS Best Practise Advice* *Organisational process design should ensure identity decisions are not be made solely based on the DVS result.* *The DVS Manager recommends that documented processes exist on how to assist with identity verification when the DVS is unavailable or a match result is not provided.*
5	**How do you integrate the DVS into your business processes to ensure that handling complaints, responding to access to information requests and reviews of decisions is**

	in accordance with the Organisation's own procedures? *DVS Best Practise Advice* *The DVS Manager recommends that user agencies should implement a well-advertised complaints handling process, supported by documentation in accordance with the Organisation's own procedures.*
6	**Confirm that your Agency's operating Interfaces with the DVS Hub are in accordance with DVS technical requirements.** *DVS Best Practise Advice* *The DVS Manager recommends that participating government agencies should:* • *Maintain and review security of connected systems in accordance with their industry, state and territory or federal security standards;* • *Ensure that any system changes to connected systems are retested in the DVS test environments prior to production implementation;* • *Update interfaces to take advantage of DVS system improvements e.g. field rationalisation; and* • *Ensure that their system is configured to protect the DVS from attack or any other behaviour that might compromise the DVS or its participants (i.e. excessive traffic).*
7	**Explain the procedures you use to promptly handle and report to the DVS Manager any suspected or actual breaches of privacy or security.** *DVS Best Practise Advice* *The DVS Manager recommends that participating Government agencies should have documented process for handling privacy and security breaches, these processes should include protocols for contacting the DVS Manager where applicable and should be provided to all relevant staff.*
8	**Have your identity decision processes been audited or reviewed since your last Compliance Statement? If so, did you report to the DVS Advisory Board any recommendations made to the Agency on improving the operation of the DVS?**
9	**How do you retain information in connection with the Agency's use of the DVS for audit and compliance purposes and to fulfil privacy and record keeping requirements including log transactions?** *DVS Best Practise Advice* *The DVS Manager recommends that participating Government agencies should maintain for 150 days audit data of transactions submitted to the DVS including:* • *timestamps when requests were sent and received;*

- *the Verification Request Number (VRN);*
- *the Originating Agency Code (OAC) ; and*
- *the document issuer identifier as per the DVS Module 6 for their IT systems.*

Physical records should be maintained for a minimum of 150 days and in accordance with applicable privacy principles.

Please provide Agency details, including:

Agency
Address:
Compliance Contact Officer:
Phone:
Email:

The Compliance Statement should be signed for and on behalf of the Agency by the **signatory of MOU/Contract (or equivalent/replacement)**

_____

Signed by:
Date:

Completion – please send to:

National Document Verification Service
Home Affairs
3-5 National Circuit
BARTON, ACT, 2600
Email: s. 22(1)(a)(ii) homeaffairs.gov.au

The Statements are considered confidential documents and will be handled and stored appropriately.

Home Affairs will consider Compliance Statements prior to them being provided to the DVS Advisory Board. Home Affairs may seek additional information to support the Statements. The Advisory Board will make recommendations on the acceptance of the Compliance Statements and will monitor that corrective action is taken on any area where Agencies fail to comply with their MOU/Contract.

Addendum 2 – Current Users

Agency Name	Senior Executive Contact	MOU contact Officer	DVS Use	Commencement Date
[Insert name of additional Agency Party to this MOU]	*[Name]* *[Position]* *[Email]* *[Contact Number]*	*[Name]* *[Position]* *[Email]* *[Contact Number]*	*[A short description of what the DVS is being used for in the organisation]*	*[Date that the Agency entered into this agreement]*

Schedule 4 – Variation Template

This form will be used to record amendments to current arrangements, including administrative, financial, technical and/or legislative aspects. Please lodge this form through the relevant Contact Officer.

Variation Request Number	Variation Number 1 of 2019 to the Memorandum of Understanding dated 13 April 2018 between the Department of Home Affairs and the Department of Veteran's Affairs (DVA).
Title	*Variation – additional document types – Visa and Immicard*
Date of Request	14 January 2019
Variation Description	In accordance with paragraph 12.1 of the MOU signed on, the MOU is varied as follows: 1. *The DVA is seeking to expand the DVS proof of identity documents that are currently validated through the MyService.* 2. *The DVA agrees to pay all connection costs to facilitate the addition of Visa and Immicards for verification to the DVS.* s. 47D s. 47D
Party Initiating Change	**DVA** ☑ **Home Affairs** ☐
Proposed Implementation Date	14 January 2019

Execution

This Variation No 1 of 2019 to the MOU dated 13/04/2018 is entered into by the Parties on the date the QLD OSR authorised delegate agrees by signing below.

Andrew Rice s. 22(1)(a)(ii)

Signed for, and on behalf of, the Commonwealth of Australia by ~~Duncan Anderson, A/g~~ Assistant Secretary, Identity and Biometrics Branch, Home Affairs, in the presence of:

s. 22(1)(a)(ii)

witness name

s. 22(1)(a)(ii)

signature of representative

s. 22(1)(a)(ii)

signature of witness

Signed by Mark Travers, Assistant Secretary, Program Integration Branch, department of Veterans Affairs, in the presence of:

s. 22(1)(a)(ii)

witness name

s. 22(1)(a)(ii)

signature of representative

s. 22(1)(a)(ii)