
# PRIVACY IMPACT ASSESSMENT

## EXTENSION OF DOCUMENT VERIFICATION SERVICE TO PRIVATE SECTOR ORGANISATIONS

For: Attorney-General's Department

20 JULY 2012

# TABLE OF CONTENTS


**1 EXECUTIVE SUMMARY ..... 4**

1.1 SCOPE OF THE PIA ..... 4
1.2 OVERALL CONCLUSION ..... 5
1.3 RECOMMENDATIONS ..... 6

**2 INTRODUCTION ..... 9**

**3 SCOPE AND METHODOLOGY ..... 10**

3.1 SCOPE ..... 10
3.1.1 Assumptions and qualifications ..... 10
3.2 METHODOLOGY ..... 11
3.3 GLOSSARY ..... 11

**4 PROPOSED CHANGES TO THE DVS ..... 13**

4.1 CURRENT OPERATION OF THE DVS ..... 14
4.2 EXTENSION OF THE DVS – PRIVATE SECTOR ORGANISATIONS AND THIRD PARTY AGENTS ..... 14
4.3 BACKGROUND TO THE PROPOSALS ..... 14
4.4 CURRENT IDENTITY VERIFICATION PROCESSES ..... 15
4.5 EXPECTED OUTCOMES AND PROPOSED PRIVACY PROTECTIONS FOR DVS EXTENSION ..... 16
4.6 ANTICIPATED PRIVACY BENEFITS OF PRIVATE SECTOR ACCESS TO THE DVS ..... 17
4.6.1 Minimise risk of identity theft and identity fraud ..... 17
4.6.2 Improve security of communications and storage ..... 18
4.6.3 reduce need for collection or storage of identity documents ..... 18
4.6.4 reduce reliance on data-scraping ..... 18
4.7 USE OF THIRD PARTY AGENTS ..... 19
4.8 ANTICIPATED PRIVACY BENEFITS OF USE OF THIRD PARTY AGENTS ..... 20

**5 ASSESSMENT OF RISKS AND RECOMMENDATIONS ..... 21**

5.1 INTRODUCTION ..... 21
5.2 OVERALL CONCLUSION ..... 21
5.3 IDENTIFIED RISKS ..... 22
5.3.1 Necessary collection ..... 22
5.3.2 openness and transparency and informed consent ..... 23
5.3.3 Security issues ..... 25
5.3.4 Accuracy of personal information ..... 26
5.3.5 Use and disclosure of personal information ..... 27
5.3.6 Limits on use of commonwealth or state unique identifiers ..... 28
5.3.7 Governance ..... 29
5.3.8 Safety net ..... 30
5.4 RECOMMENDATIONS ..... 30

**6 APPENDIX 1 – MATERIAL REVIEWED FOR THE PIA ..... 33**

**7 APPENDIX 2 – CURRENT DVS SYSTEM AND GOVERNANCE ..... 35**

7.1 DVS BACKGROUND AND OBJECTIVES ..... 35
7.2 BRIEF DESCRIPTION OF THE DVS ..... 36
7.3 DVS PARTICIPANTS AND THEIR ROLES ..... 36
7.4 OPERATING PRINCIPLES ..... 36
7.5 GOVERNANCE OF THE DVS SYSTEM ..... 38
7.6 DVS – CURRENT SYSTEM PERSONAL INFORMATION FLOWS ..... 38
7.7 COLLECTION OF PERSONAL INFORMATION ..... 41

7.8 SECURITY ..... 41
7.9 ACCURACY ..... 42
7.10 USE OF PERSONAL INFORMATION ..... 43
7.11 DISCLOSURE OF PERSONAL INFORMATION ..... 44
7.12 ACCESS AND CORRECTION ..... 44
**8 APPENDIX 3 – DATA FLOWS FOR PRIVATE SECTOR DVS USE ..... 45**
**9 APPENDIX 4 – VERIFICATION REQUEST DETAILS ..... 46**
**10 APPENDIX 5 – DETAILED PRIVACY ISSUES AND RISK ASSESSMENT ..... 47**

# 1 EXECUTIVE SUMMARY

The DVS was developed as part of Australia's National Information Security Strategy (NISS). It was designed to protect individuals' privacy by improving procedures for evaluating the accuracy of Evidence of Identity (EOI) information and to include privacy safeguards. The DVS enables authorised agencies to confirm key details contained on government-issued identity documents presented by individuals who need to establish their identity when obtaining products or services. It is a national service providing access to document checking services from all jurisdictions.

While the DVS is currently only available to government agencies, the Australian Government recently announced in its 2012-13 Budget, that the DVS would be extended to private sector users that operate under regulatory client identification obligations. This will include organisations in the banking, superannuation, financial services, transport security and telecommunications sectors.

The extended service will include the verification of Medicare cards and be run on a fee-for-service basis.

While the Budget announcement makes verifications of Commonwealth-issued documents available to business, consultations on making State and Territory-issued document checks available to businesses via the DVS are progressing with the jurisdictions.

The Australian Government is aiming to have a full service offering of Commonwealth, State and Territory credentials available by the end of 2012, with actual verifications to commence between June and September 2013.

The Attorney-General's Department (AGD) as the DVS Manager has asked Information Integrity Solutions Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) of the extension of the DVS to private sector organisations with specific legal obligations under law to identify their customers and to third party agents in the context of an principal-agent relationship.

## 1.1 SCOPE OF THE PIA

IIS was asked to prepare a PIA report identifying privacy risks, and identifying options to mitigate those risks, for the proposals within the context of existing commercial evidence of identity practices, including:

- paper-based and manual processes and
- use of data-scraping services.

The PIA assessed privacy issues on the basis of the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) in the *Privacy Act 1988* as well as broader privacy risks. Amongst other things, it has also considered:

- existing DVS policies on the use of the service and
- measures identified under the DVS private sector proposal to:
    - improve privacy and information security outcomes and

- strengthen compliance and transparency on DVS use.

## 1.2 OVERALL CONCLUSION

As a key plank in Australia's NISS the DVS aims to assist organisations to make good decisions in relation to their identity verification obligations by providing input to the process. Importantly, decisions about client or customer identity remain entirely with the User Organisation.

In making its privacy impact assessment IIS has noted a number of system and management features of the DVS that have been consciously designed in to minimise privacy risks.[1] In particular, the DVS design and system emphasises informed consent, requires the DVS Hub Manager to ensure that the DVS Hub is logically separate from any other system it holds or manages, limits the role of the DVS Hub to facilitating the transfer of information and avoids the creation of any new databases. The DVS is also subject to a clear, detailed governance regime covering:

- decision-making, management and oversight
- DVS policy and procedures
- authorising new Issuer or user agencies, including opportunity for all existing Issuer agencies to consider an application
- monitoring of compliance
- risk management and auditing, including some independent monitoring by the OAIC or possibly, for the private sector organisations, contracted auditors and
- incident reporting and management.

In addition to the features noted above, additional measures are proposed for the private sector extension of the DVS. These measures include:

- limiting access by private sector organisations to those that have a demonstrable legal obligations to identify their customers and are subject to the Privacy Act and
- limiting access to third parties to where there is a clear principal-agent relationship between the User Organisation and the agent.

Following its analysis applying the core elements of the NPPs, and other sets of privacy principles, and taking into account the privacy protective features of the DVS, IIS has not identified any "show stopping" privacy issues, either in terms of compliance with privacy principles for the DVS participants or wider privacy risks or impacts for individuals.

Nevertheless, the proposals under consideration will open the DVS up to more users – over 17,000 organisations have legal obligations to verify the identity of their customers or clients – and a new model of access (principal/agent with the agent connecting directly to the DVS) and therefore, as is proposed, the expansion should be closely managed and monitored.

[1] See Appendix 2 of this document

IIS also encourages the DVS Manager to consider opportunities to promote privacy practices facilitated by the use of the DVS, such as reducing the number of identity documents needed to be satisfied of a person's identity to the required risk level and/or reducing the physical retention of copies of documents.

IIS has identified a number of areas where it considers the existing protections could be strengthened, including in relation to:

- the transparency of the process to individuals and therefore their ability to provide "informed consent" or to have problems resolved
- the collection by some Issuer Agencies of the identity of the User Organisation – while IIS appreciates that this occurs in the context of the User Agency's view of their obligations to protect the personal information in their custody, there is at least the perception of risk of use of the information for new purposes or to track individuals' activities

IIS also considers that from a policy perspective it will be important for the impact of these changes to the DVS on the overall identity verification eco-system to be monitored; this is particularly relevant as Australia, in line with many overseas countries, is now considering the need for a national trusted identities framework. It also considers that privacy impacts would need to be considered carefully if there are proposals to expand the circumstances in which private sector organisations would be permitted to access the DVS or if there are other significant changes to the DVS.

## 1.3 RECOMMENDATIONS

IIS makes the following recommendations to mitigate the risks discussed above.

**Recommendation 1 – Necessary Collection**

IIS recommends that, unless there is a clear justification for other approaches, the DVS system in all cases will advise Issuer Agencies that the source of a verification request is the DVS Hub and will not identify the User Organisation.

**Recommendation 2 – Informed Consent, Privacy Notices and Openness**

IIS recommends that:

- the application for private sector organisations to access to the DVS explicitly requires customers to have given "informed consent"
- the DVS arrangements include a requirement in online applications for individuals to have the opportunity to provide separate express consent for each document to be checked
- the DVS Manager investigates consent and privacy notice best practice including consulting with community and privacy stakeholders at appropriate points and revise the consent/notice requirements as needed.
- the DVS Manager encourages all Users (and Issuer Agencies) to have material available, for example in a privacy policy, on their use of the DVS that includes:

- an explanation in broad terms of the DVS, including the information flows, the DVS participants and their roles
- how a person can deal with problems in relation to an identity verification process, including if there may be problems with their documents and about complaint processes
- an explanation of how informed consent is obtained and, where an agent is used in a client enrolment or other identity checking processes, who is dealing with the customer and collecting consent.

**Recommendation 3 – Security**

IIS recommends that:

- to support the DVS Advisory Board's consideration of private sector Organisations' applications to use the DVS, the DVS Manager should investigate possible privacy criteria or indicators
- the DVS Manager should ensure that there is an active focus on risk assessment and monitoring as private sector Organisations come on board and use the DVS
- the DVS Manager should review the private sector application and Terms and Conditions of use and the DVS supporting material (including the contract) to ensure that security incidents which are relevant to the organisation's use of the DVS, including those involving personal information, are reported to the DVS Manager, and actioned, as soon as possible
- in line with privacy good practice and to complement the existing DVS incident reporting scheme, the DVS system adopts the Office of the Information Commissioner's *Data breach notification - A guide to handling personal information security breaches,* requiring the DVS Hub Manager, and User organisations, (and User and Issuer Agencies) to advise affected individuals in the event of a data security breach that occurs in the context of a DVS check or from the DVS Hub.

**Recommendation 4 – Accuracy**

IIS recommends that:

- the DVS Manager should encourage User Organisations, where they receive a No or Error response, to check data entry including the rules for a particular document before moving to another document
- the DVS Manger should monitor the frequency and nature of error messages in the system as a whole and for particular organisations and take action as needed
- the DVS Manager should ensure that there is readily available information for individuals about the DVS and when it might be appropriate for them to approach an Issuer Agency to have an issue resolved and which provides some point of contact, which might be the

Privacy Commissioner, if the individual is unable to find out if an application failed because of a problem with an identity document.

**Recommendation 5 – Monitoring use of DVS information**

IIS recommends that the DVS Manager should monitor use of the DVS to identify and respond to any trends to use DVS results for new or unexpected purposes.

**Recommendation 6 – Governance**

IIS recommends that:

- the DVS Manager and other relevant bodies in the DVS governance arrangements should monitor the implementation of the extension of the DVS to private sector Organisations and to third party agents to identify any new or unexpected privacy risks and to ensure that appropriate levels of monitoring are maintained regardless of the scale of the expansion
- the DVS Manager ensures that private sector User Organisations are subject to a regular cycle of independent audits, whether by the OAIC or by contracted auditors
- any extension of private sector DVS access, beyond the current proposals for access, where private sector organisations have demonstrable legal obligations to identify their customers and to third party agents in the context of an agent-principal relationship, should be the subject of a privacy impact assessment, which includes consultation with community representatives and privacy advocates
- any other significant changes to the DVS, for example any changes in the information held by the DVS Hub, should be subject to similar privacy impact assessments
- the arrangements be subject to a review after three years of operation to establish that they are operating as anticipated and that there is no unexpected impact on privacy.

**Recommendation 7 – Safety Net for individuals**

IIS recommends that the DVS Manager monitors the DVS arrangements, including through consultation with community and privacy representatives, to ensure that the processes by which an individual could seek to resolve issues are clear and do not result in a complaint “merry go round”.

# 2 INTRODUCTION

The Attorney-General's Department (AGD) has asked Information Integrity Solutions Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) of the recently announced extension of the National Document Verification Service (DVS) to certain private sector organisations authorised or required under law to identify their customers and to third party agents in the context of an agent-principal relationship.

The Government expects considerable benefits from private sector initiative including:

- better privacy protection for individuals by minimising the copies of documents held
- better protection from identity fraud
- that the service will strengthen personal identity data holdings in the private sector and
- that it will also save business money by reducing unnecessary manual processes, data collection and recordkeeping.

The DVS has been operational in its current form since 2008. The Office of the Privacy Commissioner (OPC) (now Office of the Australian Information Commissioner (OAIC)) has been funded to conduct regular audits of the DVS during the development and implementations phases from 2007. In May 2009 OAIC completed a DVS Information Privacy Principle (IPP) audit that found that the DVS "affords an opportunity to implement an enhanced privacy practice model for the handling of personal information associated with the verification of [evidence of identity] EOI documents."[2]

This PIA is being undertaken as part of the Australian Government's commitment to ensuring that privacy considerations are reflected in the continued development of the DVS Project. It considers both the benefits in extending access to the DVS to specified private sector organisations and the potential privacy risks. Where risks are identified the report includes recommendations to mitigate the risks.

[2] Office of the Privacy Commissioner, *National Document Verification Service: Department of Foreign Affairs and Trade, Department of Immigration and Citizenship, ACT Department of Births Deaths and Marriages, ACT Road User Services and Centrelink: Final Audit Report: Information Privacy Principles Audit*, Sydney May 2009

# 3 SCOPE AND METHODOLOGY

## 3.1 SCOPE

IIS was asked to prepare a PIA report identifying privacy risks, and identifying options to mitigate those risks, related to:

- extending use of the DVS to private sector organisations in specified circumstances and
- permitting third party agents to access the DVS in the context of an agent/principal relationship, through the IT systems of their principal or by direct connection to the DVS.

The report assesses privacy risks of private sector use of the DVS within the context of existing commercial evidence of identity (EOI) practices, including:

- paper-based and manual processes and
- use of data-scraping services.

The report takes into account:

- the draft PIA material prepared by AGD
- measures identified under the DVS private sector proposal to:
    - improve privacy and information security outcomes and
    - strengthen compliance and transparency on DVS use
- existing DVS policies on the use of the service and
- the privacy implications of private sector DVS use in the context of the proposed revisions to the national privacy regime set out in the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Privacy Amendment Bill).

The PIA was conducted on the proposal to extend the DVS and was based on policy papers, project and system documentation and discussions with AGD staff. At this point in the project, and given the time available, external stakeholder consultation has not been undertaken.

### 3.1.1 ASSUMPTIONS AND QUALIFICATIONS

The following assumptions and qualifications were applied as the PIA was undertaken:

- that it was not necessary or efficient to focus in detail on every possible privacy risk; rather, it is better to focus on the most critical issues
- the PIA considered the risks for all participants in the DVS system but used the National Privacy Principles (NPPs) in the *Privacy Act 1988* (the Privacy Act) as the basis for the analysis and has not considered in detail the different privacy laws that are applicable to the participants in different jurisdictions

- the assessment and recommendations in this report are intended as general policy advice; they are not intended to be and should not be taken as legal advice.

## 3.2 METHODOLOGY

In conducting this PIA IIS worked closely with the relevant AGD staff. The approach applied is based on the OAIC's *Privacy Impact Assessment Guide* 2010.[3] IIS also drew on other current PIA best practice in Australia and internationally, as well as its own framework for analysis and solution identification.

In undertaking this PIA, IIS took the following steps:

- gathered information about the DVS and the proposed extension of the service to specified private sector organisations – a list of the material reviewed is at Appendix 1
- read and analysed the data, considering the issues from the perspective of the various participants in the DVS and using the NPPs in the Privacy Act as the analytical framework. The analysis also drew on the IPPs in the Privacy Act, on key variation in the privacy principles in other jurisdictions, as well as the proposed Australian Privacy Principles (APPs) in the Privacy Amendment Bill, and also wider privacy challenges including the fair allocation of risks between organisations and individuals
- prepared a draft report for comment by AGD and
- finalised the report based on feedback received.

## 3.3 GLOSSARY

| Term or abbreviation | Meaning |
|---|---|
| AGD | Attorney-General's Department |
| Agency | Commonwealth, State or Territory Government Agency |
| APPs | Australian Privacy Principles (*proposed*) |
| DVS | National Document Verification Service |
| DVS Hub | DVS Hub that securely directs requests between User and Issuer Agencies. The Hub does not retrieve any information held by the Issuer Agency. |
| EOI | Evidence of Identity |
| IGA | Intergovernmental Agreement |
| IPP | Information Privacy Principle in the Privacy Act |

[3] Available at http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html

| Term or abbreviation | Meaning |
|---|---|
| ISIDRAS | Information Security Incident Detection, Reporting and Analysis Scheme |
| Issuer Agency | The agency which issued the document and has agreed to provide an automated verification service for DVS requests submitted by User Agencies |
| NISS | National Identity Security Strategy |
| NISCG | National Identity Security Coordination Group |
| NPPs | National Privacy Principles in the Privacy Act |
| OAC | Originating Agency Code |
| OAIC | Office of the Australian Information Commissioner |
| OPC | Office of the Privacy Commissioner |
| MoU | Memorandum of Understanding |
| Privacy Act | *Privacy Act 1988* |
| Privacy Amendment Bill | *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* |
| User Organisation | The querying organisation authorised to utilise the DVS to verify details on identity documents issued by Issuer Agencies |
| VRN | Verification Request Number |

# 4 PROPOSED CHANGES TO THE DVS

This PIA considers two proposed changes to the DVS:

- extending use of the DVS to private sector organisations that have a demonstrable legal obligation to identify people – potentially some 17,000 organisations – and
- permitting third party agents to access the DVS in the context of an agent/principal relationship, through the IT systems of their principal or by direct connection to the DVS.

The identity verification requirements for private sector organisations arise, for example, under legislation and related regulations:

- in the financial services sector under various provisions such as those found in the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* [4], the *Superannuation Industry (Supervision) Regulations 1994* and the *Credit Reporting Code of Conduct* made under the Privacy Act
- in the telecommunications sector, under regulations made under subsection 99(1) of the *Telecommunications Act 1997,* carriage Service Providers and their retailers are required to collect and verify their customer's identity and address information [5][6]
- in the transport, sector Individuals wishing to work in secure aviation or maritime zones need to apply for an Aviation Security Identification Card (ASIC) or a Maritime Security Identification Card (MSIC). Applicants need to provide documents to prove their identity and Australian citizenship or residency. ASIC and MSIC cards are only issued after the issuing body has established the applicant's identity and background checks are conducted as required under the Aviation Transport Security Regulations 2005 made under the *Aviation Transport Security Act 2004*, and the *Aviation Transport Security (Consequential Amendments and Transitional Provisions) Act 2004* and the Maritime Transport and Offshore Facilities Security Regulations 2003 made under the *Maritime Transport and Offshore Facilities Security Act 2003*[7][8][9]

---

[4] *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006, Part 2 – Identification Procedures Etc., http://www.austlii.edu.au/au/legis/cth/consol_act/alacfa2006522/.

[5] *Telecommunications Act 1997* – Telecommunications (Service Provider – Identity Checks for Pre-paid Public Mobile Telecommunications Services), http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrumentCompilation1.nsf/0/4CC0EE2AD34B6DB6CA25701A002074D2/$file/IDChksPrePaidMob.pdf.

[6] Australian Communications and Media Authority, *Pre-paid mobile phone services - industry information collection fact sheet*, Canberra, February 2010, http://www.acma.gov.au/WEB/STANDARD/pc=PC_507.

[7] Department of Infrastructure, Transport, Regional Development and Local Government, *Fact Sheet 13: Aviation Security Identification Cards (ASICs)*, Canberra, May 2010, http://www.infrastructure.gov.au/transport/security/aviation/factsheet/fact13.aspx

[8] Department of Infrastructure, Transport, Regional Development and Local Government, *Strengthening Maritime Security: Understanding our security responsibilities*, Canberra, 2008, 33, <http://www.infrastructure.gov.au/transport/security/maritime/pdf/Strengthening_MarSec_Guide_2008.pdf>.

[9] *Aviation Transport Security Act 2004* and the *Aviation Transport Security (Consequential Amendments and Transitional Provisions) Act 2004*, Aviation Transport Security Regulations 2005 - Select Legislative Instrument 2005 No. 18 as amended, http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrumentCompilation1.nsf/0/A2B607B22464C266CA25776500837717/$file/AviationTransportSecurityRegulations2005.pdf.

The questions for this PIA are whether extending DVS in these ways would lead to new or increased privacy risks to personal information and/or the DVS and, if so, whether these risks could be effectively mitigated.

## 4.1 Current operation of the DVS

The DVS plays a role in improving identity security by facilitating electronic verification for government agencies. It facilitates a process where a User Organisation seeks confirmation from an Issuer Agency (a federal or State or Territory body that issues document such as a passport or drivers licence) that a document presented is valid. The DVS is designed to strengthen and support identification and registration processes by providing users with greater certainty about the validity of identity documents presented by individuals. The DVS, as a highly automated process, is also able to support the strong trend to on-line transactions; in most cases individuals will not need to present documents, or undergo further identity verification processes, in person.

An overview of the DVS as it currently operates is at Appendix 2. It is an administratively established program. It does not have governing legislation but is run under a detailed set of governance arrangements, starting with the Council of Australian Governments (COAG) and the National Identity Security Coordination Group (NISCG), which includes the Federal Privacy Commissioner's representative. For this PIA it is important to note that the DVS has been designed, amongst other things, to minimise its impact on the privacy of individuals. Two key design features worth noting here are that:

- the DVS check simply returns a "Yes", "No" or "Error" message and does not return any additional information about the individual and
- the DVS Hub simply facilitates the transfer of the request and response and, once the transaction is complete, does not retain any record of the transaction, including in audit logs or other IT records, that would allow the DVS Hub Manager to have any knowledge of the identity of the individual or the document that has been verified.[10]

## 4.2 Extension of the DVS – Private sector organisations and third party agents

To date, the DVS has been restricted to government users; use of the DVS is being progressively taken up across Commonwealth, State and Territory agencies. As information has become available concerning the operation of the DVS, private sector organisations have requested access to enhance their EOI procedures. Like government agencies, in particular circumstances private sector organisations must be able to accurately identify individuals, whether they are customers or employees. It is important to note here that NPP 8 in the Privacy Act requires organisations to permit individuals to interact with them anonymously where it is lawful and practicable; there is no across the board requirement to identify individuals.

## 4.3 Background to the proposals

The DVS is a key element of COAG's National Information Security Strategy (NISS) and is designed to underpin strengthened decision-making on the EOI presented by people seeking services or benefits.

[10] The DVS does keep records for billing, audits etc. The audit information will include Virtual Reference Number(s), requesting agency, document type, verification response (including any error code), and date-time stamps.

In November 2009 the NISCG identified extension of the DVS to the private sector as a key strategic priority for the future of the NISS.

Since then AGD, in consultation with DVS Advisory Board members, has been developing proposals starting with the extension of verifications services for Commonwealth documents to authorised commercial organisations.

In September 2011, the Commonwealth Attorney-General wrote to premiers and first ministers seeking in-principle approval from the jurisdictions and feedback identifying any potential legislative work required to realise private sector access to the full national DVS; IIS understands that all jurisdictions, bar one, have provided the Attorney-General with their in-principle policy approval for the proposal.

Following further consultation with all jurisdictions, in May 2012, the Australian Government approved the commercial extension of the DVS and provided a funding allocation as part of the 2012-13 Budget to cover set-up costs for the new service including the addition of Medicare card verifications.

AGD anticipates that subject to negotiations with the States and Territories, it would be possible to accept the first applications from the private sector from the end of this year, with the first credentials being verified as early as June 2013.

## 4.4 Current Identity verification processes

IIS understands that currently it is common practice in the private sector for identity documents that are provided by an individual to be largely accepted at face value. Documents are routinely copied by organisations and the copies are retained in hard or scanned form.

An organisation may seek additional documentation where it is not satisfied that the individual has established his/her identity to a sufficient level. This might include manual, or in some cases online (through subscription to the document issuers' database), verification of personal information. Manual document verification by an organisation of papers presented to it involves the organisation forwarding personal information to the document Issuer Agency by mail, fax, email or transcribing it over the phone. The Issuer Agency will then undertake a manual search of its registers and usually respond with a copy of the document or additional supporting detail about the applicant. Online verification can involve for example, CertValid (the Certificate Validation Service), which verifies Birth, Marriage and Change of Name Certificates issued by State and Territory Registries, or the Visa Entitlement Verification On-line service, which is operated by the Department of Immigration and Citizenship to allow organisations to verify visa details. [11] [12]

Organisations in the finance sector have recourse to other service providers such as credit reference agencies to undertake checks on their behalf. In 2009, the Anti-Money Laundering Magazine identified the public and proprietary data sources used to conduct checks:

- The Australian Electoral Roll,

[11] The CertValid system is operated at the NSW Registry of Births Deaths and Marriages for all State and Territory Registries.
[12] Visa Entitlement Verification On-line service is operated by the Department of Immigration and Citizenship.

- Sensis White Pages,
- Department of Immigration and Citizenship,
- Department of Foreign Affairs and Trade watchlists,
- Australia Post Postal Address file, and
- Proprietary databases such as historical white pages, an online public number directory derived from Telstra's Integrated Phone Number Directory and other in-house credit reference data.[13]

A number of organisations providing identity verification services also include "data-scraping" as part of the services they offer. A form of web harvesting, data-scraping obtains validations of client data from a service agency's public-facing internet facilities by:

- encouraging a client to provide authentication details and logon data into an online account or service portal, and
- running third-party systems that can observe and register the results of that transaction. A successful login is then recorded as successful client verification and sold onto a client organisation.

## 4.5 Expected outcomes and proposed privacy protections for DVS extension

The first proposal under consideration is to extend access to the DVS to private sector organisations in specified circumstances. When integrated into a business process, the DVS is intended to allow organisations to:

- verify EOI documents issued by government agencies across Australia
- replace cumbersome and expensive manual processes, wherein only a small fraction of documents are verified
- conduct more checks more accurately on key EOI documents, providing greater confidence in the identity of the applicant, thereby strengthening registration and reducing the risks of identity theft or fraud
- avoid the need for separate access negotiations with a variety of document issuing authorities and otherwise gain cost and time efficiencies for themselves and for individuals through a responsive, reliable, automated process
- improve public confidence in the use and protection of personal information and
- comply with legislative requirements.

A diagram of the information flows that would be involved in private sector access to the DVS is at Appendix 3.

[13] Adam Courtenay, 'Survey of Electronic Verification Service Providers' (May 2009) *Anti-Money Laundering Magazine*, 14 – 21 www.amlmagazine.com.au.

IIS understands that the following measures are to be included to ensure that the extension of the DVS as proposed does not introduce new privacy risks:

- generally the Issuer Agencies will not be aware of the source of the verification request; the source of a verification requests is presently only provided to Registries of Births Deaths and Marriages, as specifically requested by them
- access to the DVS will be limited to those private sector organisations:
    - with demonstrable legal requirements to identify individuals using their services or products and
    - that are subject to the Privacy Act
- use of the DVS will be limited to the verification of identity documents as part of an organisation's application or registration processes and to meet identity verification obligations
- Organisations seeking to use the DVS will be subject to a formal application process – the application will be approved by the DVS Advisory Board
- access to the DVS will be subject to contracts with the Commonwealth setting out the terms of participation, including requirements to:
    - comply with the Privacy Act
    - abide by the standards and protocols governing DVS administration, access and use as set out in the DVS Supporting Material and
- undergo audits of their use of the DVS undertaken either by OAIC or by contracted auditors.

IIS understands that AGD is also considering whether there should be a requirement in online applications for individuals to have the opportunity to provide consent for each document to be checked, rather than providing blanket consent to a range of DVS checks.

## 4.6 ANTICIPATED PRIVACY BENEFITS OF PRIVATE SECTOR ACCESS TO THE DVS

The extension of the DVS to private sector organisations as proposed seems likely to have a range of privacy benefits as follows.

### 4.6.1 MINIMISE RISK OF IDENTITY THEFT AND IDENTITY FRAUD

Current EOI processes often involve acceptance of identity documents at face value. IIS understands that reliance on photocopied documents (certified or otherwise) is also common. The DVS enables authorised organisations to confirm key details contained on government-issued identity documents presented by individuals, adding to the assurance that the documents presented have not been fabricated, or otherwise tampered with, or are no longer valid (possibly because they were lost or stolen).

### 4.6.2 IMPROVE SECURITY OF COMMUNICATIONS AND STORAGE

The DVS offers more secure communications than the current online or manual processes. IIS also understands that many private sector EOI transactions remain paper-based involving document handling, copying and manual storage procedures. Unless managed well there are considerable privacy and security risks in such manual processes. For example, IIS understands that in the SIM card retail context, regulators and law enforcement agencies often report "shoebox filing". Large quantities of personal data and documents are photocopied and collected as part of a prepaid mobile purchase and this material is often simply kept in boxes or piles stored behind shop counters.

### 4.6.3 REDUCE NEED FOR COLLECTION OR STORAGE OF IDENTITY DOCUMENTS

EOI policies have historically developed to establish assurance about a client's identity through accumulating a "footprint" of identifying documents. For example, if a bank has any doubts about the identity of a client, anti-money laundering regulations encourage the collection of more personal information from the client. This is resulting in large amounts of personal information, documents and other data being collected for a range of key financial products and services. The DVS offers the opportunity to reduce privacy risk through electronic data checks that might obviate the need for the accumulation of extensive personal data for identification purposes.

The Attorney-General's Department's industry consultations on expanding use of the DVS indicate many organisations foresee greatly reducing their recordkeeping burden by replacing existing paperwork with an electronic record of a DVS check with receipt details of that transaction, which include a unique transaction number, the document type, the match result and the date and time details for that transaction.

Recent statements by Timothy Pilgrim, Federal Privacy Commissioner have underlined the privacy risks inherent in the increasing amounts of personal information being collected by private sector organisations. Commissioner Pilgrim has noted that the scale of personal information being collected can pose a significant privacy exposure to both the organisations and its customer. In this context, extending the DVS to the private sector could help mitigate privacy risks to both individuals and businesses.[14]

### 4.6.4 REDUCE RELIANCE ON DATA-SCRAPING

The absence of alterative online identity checking options, including matching document details to the Issuer Agency's database via the DVS, have seen the emergence of the "data-scraping" mentioned above.

Data scraping operates outside an authorisation by or formal agreement with that service agency and exploits that agency's customer service portal often to the detriment of that service portal's intended purpose. There are also concerns data scraping techniques provide technical access into client accounts and facilities by parties other than the client, for example validations sourced through Medicare online account applications.

[14] The Brisbane Times 14 July 2012 accessed at http://www.brisbanetimes.com.au/business/every-click-you-make-theyll-be-watching-you-20120713-221ay.html

## 4.7 USE OF THIRD PARTY AGENTS

The NISCG has endorsed use of the DVS by User Organisations' third party agents acting upon on their principal's behalf.

The agreed Third Party Access Policy is aimed at addressing the increasing trend in government and businesses to outsource components of their business, in this case identity processing. An agent is now able to make a technical connection via the principal organisation, or direct to the DVS Hub. If a third party agent is servicing, or will service, several DVS User Organisations or Agencies, the optimal operational arrangement is for a single connection by the third party directly to the DVS Hub. This will reduce complexity for DVS operations and for User Organisations or Agencies, resulting in lower cost to both.

IIS understands that the third party access policy places requirements on all DVS Users (including government agencies or potential private sector organisations) intending to have an agent access the DVS on their behalf. These conditions include:

- providing advance notification of entry into a third party DVS arrangement to the DVS Advisory Board
- confirming that the contractual arrangement with agent is one of principal and agent by providing transparency regarding the terms of the principal-agent relationship (i.e. contractual terms relevant to DVS use)
- ensuring that an organisation's agent's use of its DVS access will be consistent with the DVS use and access conditions, detailing the contractual measures ensuring the agent's compliance
- providing additional material as part of the Annual Compliance Statement including any updates or modifications to the User Organisation's risk management plan to enable its agent's use of the DVS
- obtaining agreement of the agent to audits of compliance with the terms and conditions of DVS access being conducted by the OAIC or an independent auditor
- other measures required of the principal and agent if the agent was to connect direct to the DVS, rather than via a User Organisation's IT System include:
    - agents would sign binding terms with the DVS Manager regarding its technical connection
    - modification of the User's agreement with its agent to add additional requirements that relate to the DVS, including compliance mechanisms
    - business segregation measures required of the agent to ensure that the DVS is used only to verify clients of authorised DVS Users
    - due diligence undertaken by the User to ensure that their agent has effective measures in place to quarantine their work, prohibiting DVS verifications being

carried out on behalf other non-DVS User organisations' clients (business segregation)

- agent subjects itself to monitoring/ auditing by the Principal and independent auditors and
- an IT connection through the approved DVS channel to the DVS Hub at Centrelink

## 4.8 ANTICIPATED PRIVACY BENEFITS OF USE OF THIRD PARTY AGENTS

This proposal is likely to yield direct benefits in terms of cost savings for organisations, and individuals, involved in identity verification processes. There will be economies of scale and less steps or participants in the process.

The proposed management arrangements should also mean that use of agents in the DVS process will be transparent and subject to appropriate safeguards and supervision.

Expanding DVS access to third party agents is also likely to support other proposed changes to the DVS system, in particular, the proposed extension to allow private sector organisations to access the DVS. Organisations with a smaller customer base, or with an eye to efficiencies, may be more inclined to use the DVS if there were a range of already connected agents in place to support the move. In turn, there is likely to be less collection of personal information and less manual handling and storage.

The increased flexibility should also allow for a greater level of client driven transactions and choice.

# 5 ASSESSMENT OF RISKS AND RECOMMENDATIONS

## 5.1 INTRODUCTION

This PIA has a focussed scope in that it is assessing two specific proposed changes to the DVS, not the operation of the DVS system as a whole. This section of the report sets out IIS's overall conclusions in relation to the two proposals, the privacy risks identified and recommendations to mitigate those risks.

## 5.2 OVERALL CONCLUSION

The DVS provides the service of matching key details contained on EOI documents against the records of the authority that issued the document. As a key plank in Australia's NISS it aims to assist organisations to make good decisions in relation to their identity verification obligations by providing input to the process. Importantly, decisions about client or customer identity remain entirely with the User Organisation.

In making its privacy impact assessment IIS has noted a number of system and management features of the DVS that have been consciously designed in to minimise privacy risks.[15] In particular, the DVS design and system emphasises informed consent, requires the DVS Hub Manager to ensure that the DVS Hub is logically separate from any other system it holds or manages, limits the role of the DVS Hub to facilitating the transfer of information and avoids the creation of any new databases. The DVS is also subject to a clear, detailed governance regime covering:

- decision-making, management and oversight
- DVS policy and procedures
- authorising new Issuer or User Agencies, including opportunity for all existing Issuer Agencies to consider an application
- monitoring of compliance
- risk management and auditing, including some independent monitoring by the OAIC or possibly, for the private sector organisations, contracted auditors and
- Incident reporting and management.

In addition to the features noted above, additional measures are proposed for the private sector extension of the DVS. These measures include:

- limiting access by private sector organisations to those that have a demonstrable legal obligations to identify their customers and are subject to the Privacy Act and
- limiting access to third parties unless there is a clear principal-agent relationship between the User Organisation and the agent.

[15] See Appendix 2 of this document

Following its analysis applying the core elements of the NPPs, and other sets of privacy principles, and taking into account the privacy protective features of the DVS, IIS has not identified any "show stopping" privacy issues, either in terms of compliance with privacy principles for the DVS participants or wider privacy risks or impacts for individuals.

Nevertheless, the proposals under consideration will open the DVS up to more users – around 17,000 organisations are understood to have demonstrable obligations to verify the identity of their customers or clients – and a new model of access (principal/agent with the agent connecting directly to the DVS) and therefore, as is proposed, the expansion should be closely managed and monitored.

IIS also encourages the DVS Manager to consider opportunities to promote privacy practices facilitated by the use of the DVS, such as reducing the number of identity documents needed to be satisfied of a person's identity to the required risk level and/or reducing the physical retention of copied of documents.

IIS has identified a number of areas where it considers the existing protections could be strengthened, including in relation to:

- the transparency of the process to individuals and therefore their ability to provide "informed consent" or to have problems resolved
- the collection by some Issuer Agencies of the identity of the User Organisation – while IIS appreciates that this occurs in the context of the User Agencies' view of their obligations to protect the personal information in their custody, there is at least the perception of risk of use of the information for new purposes or to track individuals' activities

IIS has expanded on the risks in the section below and makes recommendations to mitigate these risks.

IIS also considers that from a policy perspective it will be important for the impact of these changes to the DVS on the overall identity verification eco-system to be monitored; this is particularly relevant as Australia, in line with many overseas countries, is now considering the need for a national trusted identities framework. It also considers that privacy impacts would need to be considered carefully if there are proposals to expand the circumstances in which private sector organisations would be permitted to access the DVS or if there are other significant changes to the DVS.

## 5.3 IDENTIFIED RISKS

This section of the report sets out the key privacy risks identified following the analysis set out in the table in Appendix 5.

### 5.3.1 NECESSARY COLLECTION

Limiting collection is the first level of defence in the protection of personal information; generally personal information should be collected only where it is necessary for an organisation's lawful functions and activities.

As noted the DVS system is designed to limit the collection of personal information.

IIS understands that generally, Issuer Agencies will not be notified as to the source of a verification request (the message will simply indicate that it has been sent by the DVS Hub). However, it also understands that some Issuer Agencies (Registrars of Births, Deaths and Marriages) consider their governing legislation requires them to know the User Organisation so they can, if requested, advise the individuals concerned to whom a verification response was provided.

IIS considers that the possible privacy benefits here are outweighed by the potential risks. This is particularly the case given that the DVS is intended to operate on the basis of informed consent. The process of giving consent should mean that that the individual is already aware that a check with the Issuer Agency will be undertaken and a response provided (therefore there appears to be little gain for individuals if the Issuer Agency knows the source of the request). IIS also understands that the DVS logging requirements mean that in the event of complaints or other issues that the DVS Hub Manager, or the DVS Manager, can reconstruct the transaction should an Issuer need to learn the origin of a verification message, for example for a freedom of information request.

The risks to privacy on the other hand have the potential to be significant. Over time Issuer Agencies that collect information about the source of the request could build up a rich picture of an individuals interactions with government and private sector organisations. It is increasingly being recognised that "Data grows ever more connected and valuable with use. Connecting two pieces of data creates another piece of data and with it new potential opportunities (as well as new potential harms)".[16]

IIS encourages further consideration of the need to collect information about the User Organisation.

### 5.3.2 OPENNESS AND TRANSPARENCY AND INFORMED CONSENT

Privacy principles aim to put individuals in control of personal information about them by ensuring they know what information is collected and why and how it is handled. The requirements, with some variations between jurisdictions, include giving some information at the point of collection and supporting this with some readily available information about the sort of personal information the organisation holds. Some jurisdictions require a detailed privacy policy on information handling practices; for example, NPP 5 of the Privacy Act requires organisations to have a privacy policy and to make it available on request. Informed consent may also be required in some cases, for example, for the collection of sensitive information.

The DVS operates on the basis that verification checks are subject to individual consent. IIS understands that part of the DVS Advisory Board's assessment of a potential User is consideration of the adequacy of their consent process (is it clear, is it informative etc); review of forms and feedback from Issuer Agencies has seen changes to a number of agencies disclosure statements. User Organisations (as User Agencies already are) will also be required to confirm, annually, that they comply with relevant laws including privacy laws.

While these measures are welcome, IIS considers that the consent process is critical to the ability of individuals to make informed choices about a DVS check. It has identified some areas that could be

[16] For example see papers on the subject of big data at http://www.weforum.org/reports/personal-data-emergence-new-asset-class and http://www.weforum.org/issues/rethinking-personal-data/

strengthened and it also encourages the DVS Manager to continue to investigate good practice in this area.

The points of risk that IIS has identified are as follows:

- The draft application, and terms and conditions for private sector User Organisations do not currently specifically mention the need for individual consent. While there is a requirement to comply with all relevant laws, it is important to note that private sector organisations are subject to the NPPs in the Privacy Act; the NPPs only requires consent to collect or disclose personal information in specified circumstances (sensitive information, unrelated disclosures). While all the supporting material, including the yearly DVS compliance statement that will require User Organisations to report on privacy matters including consent, emphasises consent there is at least room for ambiguity about the enforceability of the consent requirement.

- While IIS understands that consent processes are reviewed, it is aware of private sector practices that are not as user friendly as they could be, for example the consent request will be in small print, bundled with other matters where consent is sought, is sought after check is conducted or does not provide sufficient, or any, information, about the DVS process or Issuer Agencies.

- There is a risk that the introduction of a third party agent into the process will affect the quality of the consent processes, particularly if is not clear the whether the Organisation (or Agency) or the agent obtains consent.

- While the current DVS supporting material does emphasise consent, it gives limited guidance on what would constitute effective consent in the context of the DVS. For example, the current Memorandum of Understanding (MoU), which governs government agencies access to the DVS, provides that agencies will take measures to seek consent and to inform individuals:

    - that the details are being collected to confirm the integrity of the Identifying Information

    - that the Identifying Information may be checked, and

    - of any legal authority under which the details of the identifying information is being collected.

IIS appreciates that there are a range of ways to meet consent and notice obligations. However, not all approaches will give an individual a clear picture of the parties involved, the information flows and uses, if any, that would be made of the information by other parties in the chain; this is likely to be particularly the case if agencies simply repeat the points from the MoU on a notice or consent form.

While the range of notice and consent practices in use are not a problem created by the DVS, IIS suggests it is an issue for the DVS Manager to consider in the extension of the DVS to private sector organisations. It also supports a requirement in online applications for individuals to have the

opportunity to provide consent for each document to be checked, rather than providing blanket consent to a range of DVS checks.

### 5.3.3 SECURITY ISSUES

Privacy principles generally require organisations and agencies to protect personal information "by such security safeguards as it is reasonable in the circumstances to take" against loss, unauthorised access, access, use, modification, or disclosure and other misuse. This requirement will be most effective if implemented and supported by appropriate governance arrangements both for User Organisations and for the DVS system as a whole, which are recognised as a legitimate cost of doing business.

IIS has observed a strong emphasis on security in the material it has reviewed for the PIA. For example, it notes that the DVS policy on the DVS use by agents requires a DVS User to demonstrate that its agent complies with the DVS MoU, DVS Supporting Material and all other applicable privacy and security obligations.

IIS also notes that the audits undertaken by the OPC/OAIC have so far only identified some minor issues (for example ensuring the live data is not used in DVS system testing, for example, in setting up a new DVS User).

IIS appreciates that the DVS system will include strong checks and balances as access to the DVS is extended to private sector organisations or third party agents. These include that:

- applications for all potential User Organisations will be scrutinised by the DVS Advisory Board
- access will be subject to detailed contractual arrangements
- the DVS Manager will oversee detailed system testing for a User Organisation prior to its connection to the system, and
- User Organisations will be required to submit yearly compliance statements and will be subject to audits, which are factored into the pricing structure.

However, the move to extend the DVS to private sector organisations may increase the likelihood of some risks or introduce new ones.

Firstly, depending on the extent to which potential User Organisations seeking to connect directly to the DVS or use agents the increase in the number of organisations to be assessed and monitored will be very significant and there may be pressure for changes in process.

There will also be an increasing diversity of organisations with different IT management approaches and possibly different approaches to staff training or risk management. Also, where a User Organisation's agent (if used) connects to the DVS direct rather than via Organisation's IT system, the Organisation will not have direct visibility of the agent's DVS activities. It will need to rely on feedback from the DVS system, in reports etc, in ensuring its agent works within the requirements. Similarly, the DVS Manager will need rely on the Organisation to carry out appropriate monitoring of its agent's activities.

IIS notes that while the DVS Advisory Board would consider privacy issues there is no specific guidance on what an assessment should look for.

IIS also notes that the while the DVS Terms and Conditions of Use for Organisations and the various supporting materials include a clear incident reporting regime, including the reporting of incidents involving personal information, at present there is no requirement for this to happen expeditiously; meaning also that the possible detriment to individuals affected by the incident is not considered expeditiously.

The current incident reporting regime does not provide for Organisations (or the DVS Hub Manger or Issuer Agencies) to notify affected individuals in the event of a data security breach. This is currently not a requirement in Australian privacy laws but is on the agenda for Australian law reform and is increasingly reflected in International privacy laws. The Federal Privacy Commissioner has recently published revised guidelines on notifying individuals in the event of a data security breach that might affect them adversely.[17] IIS encourages the DVS Manager, and participants in the DVS system to adopt the Privacy Commissioner's guidelines on a best practice basis.

### 5.3.4 Accuracy of personal information

Privacy principles recognise the potential inconvenience or real harm to individuals if inaccurate information is acted upon or passed to other bodies.

Generally, the responsibility for accuracy of information used in the decisions about identity will rest with the User Organisation and Issuer Agencies will be responsible for the accuracy of documents issued. This means that neither the DVS Manager, nor the DVS Hub Manger, would generally be involved in resolving such issues. The message for private sector Organisations wishing to access the DVS will be that use of the DVS should not replace the existing decision-making processes or responsibilities and that individuals will approach either the User Organisation or the Issuer Agency to have problems resolved.

IIS has considered the privacy risks should the Issuer Agency return a "No" or "Error" response in circumstances where there is no actual problem with the document; this is a complex issue and the best response from a privacy perspective needs careful thought.

IIS understands that anecdotal evidence indicates that in the majority of cases a "No" code will be the result of a data entry error by the User Organisation, or the individual themselves if they are making an online application. Similarly, an "Error" code might mean that the system is down or that the document, while legitimate, is not held electronically by the Issuer Organisation.

IIS also understands that where a document is not verified, the Organisation, or online application, might not explicitly advise the individual of the response but rather might simply ask for another document to be presented, or require the individual to undergo alternative identity verification processes.

The issue here is not so much the potential for decisions to be made on the basis of incorrect information; the DVS is clearly intended to support rather than replace good decision-making

[17] Office of the Australian Information Commissioner *Data breach notification A guide to handling personal information security breaches April 2012*
http://www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html

processes and IIS understands that individuals would have opportunities to verify their identity in other ways, including face to face interviews. Rather, the risk is that individuals won't know about a "No" or "Error" response or won't know if the response is as a result of a data entry error, a non-electronic document or a problem with their identity document and so might not be in a position to get a problem corrected or might waste time in trying to resolve a problem where there is none.

IIS understands that the DVS System is not encouraging the provision of document-by-document feedback to individuals because of the significant risk that this will facilitate "trawling", whereby fraudsters use attempts at online application processes to get feedback on the accuracy of details they have stolen or fabricated. This is a clear privacy risk for individuals and it would be unfortunate if the operation of the DVS increased this risk.

IIS considers that an approach is needed that ensures that the management of this risk does not make it more difficult for individuals to "pass" an identity verification process or to have any problems with identity documents easily resolved.

#### 5.3.5 USE AND DISCLOSURE OF PERSONAL INFORMATION

Privacy Principles aims to keep personal information "under control" by permitting uses or disclosures outside the purpose for which the information was collected in limited circumstances, including: where the individual would expect or has been advised of the use or disclosure; for reasonably related purposes; where the individual has consented; or where the further use is authorised by law.

IIS considers that a key factor in the minimisation of privacy risks against these principles is the limited information flows involved in the DVS process, in particular:

- use of the DVS only provides User Organisations with a Yes or No response to the personal information that is already held about an individual's documents
- issuer agencies already hold the information that is passed to them for verification and, other than in the case of BDMs discussed under "collection" above, will not be advised of the source of the request
- as the DVS currently operates there appears to be limited potential to "track" individuals, and in particular, the DVS Hub has limited "visibility" of the transactions it is passing through.

However, there is still the risk that Issuer or User Organisations might use information gained in the context of DVS access for purposes that individuals would not expect or for new purposes. This risk is often called "function creep".

OAIC raised a possible issue in its 2009 audit of the DVS supporting material, noting "it is not clear whether Issuer agencies retain personal information, received from DVS requests, in a record. If Issuer agencies retain personal information, it is not clear for what purpose they do this and

whether they could use or disclose this information further". It recommended further guidance to Issuer Agencies on this issue. [18]

There is also a possibility that use of the DVS will provide User Organisations with information on the accuracy of that individual's EOI that will then allow those organisations to place a value or greater or lesser assurance on that EOI. In other words, the fact that identity documents have been verified, may add to the business case for resale of information for marketing or other third party interests.

Another, perhaps more likely, issue is that the success of the DVS will lead to pressure for its wider use in private sector identity verification processes. It's important to note that IIS has not considered the privacy risks in an extension of the DVS in this way. It considers that possible privacy benefits and risks should be assessed before access to the DVS is extended further.

As noted, the privacy principles governing an organisations use of the DVS (NPP 7.2 and NPP 2.1) limit use and disclosure to the original purpose of collection, subject to specified exceptions. In addition, the proposals for the extension of the DVS to the private sector include some additional measures that support these requirements:

- the proposed Terms and Conditions of Use for private sector Organisations provide that they should not "collect, store or use Information Match Results for any purpose associated with the provision, or potential provision of, an information service to any person" and
- the DVS arrangements will include a "delegated use" test providing that where accessed by an agent the DVS will only be used for the identification of that principal organisation's clients.

IIS considers that there will need to be careful monitoring of the DVS use to ensure that the DVS Manager is aware of any trends for re-use of information about individuals gained from DVS use. Its recommendations on governance also address the need for further assessment should there be proposals to further amend access to the DVS or to amend the role of the DVS in significant ways affecting the handling of personal information.

### 5.3.6 LIMITS ON USE OF COMMONWEALTH OR STATE UNIQUE IDENTIFIERS

In recognition of the power of unique identifiers to match or bring together information about people gathered in different contexts, some sets of privacy principles, including the Privacy Act, limit the collection and use of such identifiers.

IIS has not identified any new risks arising from the extension of the DVS to private sector Organisation or in the use of third party agents.

Organisations using the DVS to support their client enrolment will necessarily be collecting and using unique identifiers; specifically most of the Commonwealth documents that can be verified by the DVS includes a Commonwealth-issued identifier. The use or disclosure of an identifier assigned to

[18] Paragraph 3.8.6, OAIC audit of the nine Modules developed by the AGD to guide User and Issuer agencies in their use of the DVS, undertaken in April 2009. The final audit report was issued in May 2010

an individual by an organisation is contrary to NPP 7.2 except in specified circumstances, including that "the use or disclosure is required by or authorised by or under law."

Under the current proposal, DVS access will only be granted to private sector Organisations where the law authorises or requires an identity check and third party agents will be operating under the laws applying to their principal.

### 5.3.7 GOVERNANCE

The extension of access to the DVS warrants a reconsideration of governance processes to ensure they are appropriate. IIS considers that governance arrangements are a critical plank in privacy protections and that organisations participating in the DVS system must be fully accountable for their actions through measures such as clear governance arrangements, regular monitoring and audits. It also considers that governance processes should be considered by participating organisations as a cost of operations, as they currently are in the finance sector, and should be both efficient and effective. It considers that an essential condition of use should be that Organisations as well as third party agents are subject to a regular cycle of audits for which they contribute an appropriate share of costs.

IIS considers that the current processes are quite strong and notes that thought is being given to the additional risks that might arise from access by private sector organisations or use of third party agents; some of the measures proposed have been canvassed above.

In addition, with respect to access by third party agents, IIS notes that it is proposed that this only occur in the context of a legal, principal-agent relationship, as outlined above. Contractual arrangements are expected to be in place between principal and agent to ensure that the agent undertakes client identification practices within the framework of an Organisation's applicable privacy and information security regulations and complies with DVS conditions.

IIS also considers that if and as the extension of the DVS to the private sector proceeds, that the implementation is monitored closely to ensure there are no unexpected issues or risks and that resources are available to maintain the appropriate level of monitoring whatever is the scale of the expansion.

IIS also notes that under the Privacy Act, the Privacy Commissioner's audit powers do not extend to private sector organisations, although the Commissioner may conduct an audit if invited to by the organisation. It understands that the DVS Manager is currently considering options to ensure private sector Organisations accessing the DVS will be subject to independent audits either by the Privacy Commissioner or by other suitably qualified auditors.

In earlier parts of this risk analysis, IIS noted the importance of notice and consent processes for individuals and for all participants in the DVS system. It encourages the DVS Manager to investigate current best practice in this area, including by consulting privacy or community representatives at appropriate points.

IIS also considers that the governance arrangements for the DVS should include monitoring the impact of the proposed changes to the DVS on the overall identity verification eco-system.

It also considers that privacy impacts would need to be considered carefully if there are proposals to expand the circumstances in which private sector organisations would be permitted to access the DVS or if there are other significant changes to the DVS.

### 5.3.8 SAFETY NET

An important plank in privacy protection regimes is ensuring that there are clear, and easily accessed, mechanisms for individuals to resolve issues or to raise complaints. As noted, this may be an issue particularly in relation to data accuracy and the impact of increased use of the DVS.

IIS understands that the proposal to extend DVS access to private sector Organisations would be limited to those Organisations that are subject to the Privacy Act. While this will provide some level of safety net there is a risk that the increasing complexity of the DVS system may make it harder for individuals to navigate without some form of guidance or central coordination. This may be achieved by easily accessible information on a DVS website, supported by information pointing to the website provided by DVS Users, when obtaining consent and/or discussing a failed application process with an individual. IIS considers these measures do need to be monitored to ensure that the DVS system does not make it any more difficult for individuals to resolve issues with their documents.

IIS considers that it will be important regardless of how complex the DVS ecosystem becomes that individuals are able to ascertain easily the source document and document-holding agency that may be problematic. Where individuals have a problem, they should be able to have this resolved easily.

## 5.4 RECOMMENDATIONS

IIS makes the following recommendations to mitigate the risks discussed above.

**Recommendation 1 – Necessary Collection**

IIS recommends that, unless there is a clear justification for other approaches, the DVS system in all cases will advise Issuer Agencies that the source of a verification request is the DVS Hub and will not identify the User Organisation.

**Recommendation 2 – Informed Consent, Privacy Notices and Openness**

IIS recommends that:

- the application for private sector organisations to access to the DVS explicitly requires customers to have given “informed consent”
- the DVS arrangements include a requirement in online applications for individuals to have the opportunity to provide separate express consent for each document to be checked
- the DVS Manager investigates consent and privacy notice best practice including consulting with community and privacy stakeholders at appropriate points and revise the consent/notice requirements as needed.
- the DVS Manager encourages all Users (and Issuer Agencies) to have material available, for example in a privacy policy, on their use of the DVS that includes:

- an explanation in broad terms of the DVS, including the information flows, the DVS participants and their roles
- how a person can deal with problems in relation to an identity verification process, including if there may be problems with their documents and about complaint processes
- an explanation of how informed consent is obtained and, where an agent is used in a client enrolment or other identity checking processes, who is dealing with the customer and collecting consent.

**Recommendation 3 – Security**

IIS recommends that:

- to support the DVS Advisory Board's consideration of private sector Organisations' applications to use the DVS, the DVS Manager should investigate possible privacy criteria or indicators
- the DVS Manager should ensure that there is an active focus on risk assessment and monitoring as private sector Organisations come on board and use the DVS
- the DVS Manager should review the private sector application and Terms and Conditions of use and the DVS supporting material (including the contract) to ensure that security incidents which are relevant to the organisation's use of the DVS, including those involving personal information, are reported to the DVS Manager, and actioned, as soon as possible
- in line with privacy good practice and to complement the existing DVS incident reporting scheme, the DVS system adopts the Office of the Information Commissioner's *Data breach notification - A guide to handling personal information security breaches,* requiring the DVS Hub Manager, and User organisations, (and User and Issuer Agencies) to advise affected individuals in the event of a data security breach that occurs in the context of a DVS check or from the DVS Hub.

**Recommendation 4 – Accuracy**

IIS recommends that:

- the DVS Manager should encourage User Organisations, where they receive a No or Error response, to check data entry including the rules for a particular document before moving to another document
- the DVS Manger should monitor the frequency and nature of error messages in the system as a whole and for particular organisations and take action as needed
- the DVS Manager should ensure that there is readily available information for individuals about the DVS and when it might be appropriate for them to approach an Issuer Agency to have an issue resolved and which provides some point of contact, which might be the

Privacy Commissioner, if the individual is unable to find out if an application failed because of a problem with an identity document.

**Recommendation 5 – Monitoring use of DVS information**

IIS recommends that the DVS Manager should monitor use of the DVS to identify and respond to any trends to use DVS results for new or unexpected purposes.

**Recommendation 6 – Governance**

IIS recommends that:

- the DVS Manager and other relevant bodies in the DVS governance arrangements should monitor the implementation of the extension of the DVS to private sector Organisations and to third party agents to identify any new or unexpected privacy risks and to ensure that appropriate levels of monitoring are maintained regardless of the scale of the expansion
- the DVS Manager ensures that private sector User Organisations are subject to a regular cycle of independent audits, whether by the OAIC or by contracted auditors
- any extension of private sector DVS access, beyond the current proposals for access, where private sector organisations have demonstrable legal obligations to identify their customers and to third party agents in the context of an agent-principal relationship, should be the subject of a privacy impact assessment, which includes consultation with community representatives and privacy advocates
- any other significant changes to the DVS, for example any changes in the information held by the DVS Hub, should be subject to similar privacy impact assessments
- the arrangements be subject to a review after three years of operation to establish that they are operating as anticipated and that there is no unexpected impact on privacy.

**Recommendation 7 – Safety Net for individuals**

IIS recommends that the DVS Manager monitors the DVS arrangements, including through consultation with community and privacy representatives, to ensure that the processes by which an individual could seek to resolve issues are clear and do not result in a complaint “merry go round”.

# 6 APPENDIX 1 – MATERIAL REVIEWED FOR THE PIA

| Documents Reviewed |
|---|
| 1. AGD's Privacy Impact Assessment of the National Document Verification Service June 2007 |
| 2. AGD's Draft Privacy Impact Assessment – National Document Verification Service – Provision to Private Sector Organisations Feb 2012 |
| 3. Recommendation to the National Identity Security Coordination Group that members agree to the policy proposal that a User may contract an agent to conduct DVS checks on its behalf when it abides with specified conditions |
| 4. Briefing for Privacy Authorities Australia – 11 May 2012 – which outlined the proposal to extend the DVS to private sector users |
| 5. Document Verification System – Access application form (including terms and conditions) |
| 6. Various Office of the Australian Information Commissioner (formerly Office of the Privacy Commissioner) reports on audits of the DVS.<br>a. preliminary audit of the DVS Prototype in June 2006. The final audit report was published in May 2007<br>b. an end-to-end audit of the DVS system and its implementation within participating Federal and State agencies, undertaken in February 2008. The final audit report was published in May 2009<br>c. an audit of the Department of Immigration and Citizenship's (DIAC) implementation of the DVS system, undertaken in December 2008. The final audit report was issued in March 2010<br>d. an end-to-end audit of the DVS system and its implementation within participating Federal and State agencies, undertaken in February 2008. The final audit report was published in May 2009<br>e. an audit of the nine Modules developed by the AGD to guide User and Issuer agencies in their use of the DVS, undertaken in April 2009. The final audit report was issued in May 2010<br>f. an audit to assess particular aspects of Centrelink's (now DHS) role as the operator of the DVS Hub, in particular, the audit reviewed how document verification requests and responses are managed. The final audit report was issued in June 2011. |
| 7. Document Verification Service Program Steering Committee – Terms of Reference |
| 8. National Document Verification Service Advisory Board – Terms Of Reference |
| 9. DVS – Ownership And Responsibilities |

| |
|---|
| 10. Document Verification Service - Module 6 Security Plan Version 4 – July 2011 (In Confidence) |
| 11. Document Verification Service An Overview – V1.0 February 2010 |

# 7 APPENDIX 2 – CURRENT DVS SYSTEM AND GOVERNANCE

## 7.1 DVS BACKGROUND AND OBJECTIVES

Australia has a dispersed system of identity management, which does not rely on a single credential or document to confirm the identity of an individual. None of the documents commonly used for EOI purposes is issued as an identity document. Each is issued for a specific operational purpose of the issuing authority, such as confirming a person's permission to drive, as a travel document, or as evidence that a birth has occurred. Organisations enrolling an individual for services generally require multiple documents to be produced to confirm a person is who they claim to be.

The COAG Special Meeting on Counter-Terrorism addressed the issue of identity security on 27 September 2005. The resulting communiqué noted that "the preservation and protection of a person's identity is a key concern and right of all Australians," and the heads of government agreed to develop and implement a NISS to better protect the identities of Australians.[19]

Identity fraud, which involves the use of a false or misappropriated identity, was a primary concern of Australian governments when considering the strategies to adopt under the NISS. A 2007 Australian Bureau of Statistics survey found that during the preceding 12 months, some half a million Australians fell victim to identity fraud.[20] Similarly, a national privacy survey commissioned by the OPC, also in 2007, found that:

- 9% of Australians claim to have been victims of ID fraud or theft
- 60% are concerned about becoming a victim
- 36% of Australians would not deal with a company or charity because of concerns over its protection or use of their personal information.[21]

The DVS is the centrepiece of the NISS and provides a tool to address some of the key concerns about identity security. The DVS is a national service providing access to document checking services from all jurisdictions. The DVS represents not only a way to improve identity security, but also to promote privacy protection by rendering registration procedures less open to fraud.

The DVS was designed to provide privacy safeguards and protect individuals' privacy by improving procedures for evaluating the accuracy of EOI information. The DVS enables authorised agencies to confirm key details contained on government-issued identity documents presented by individuals when seeking to establish their identity when obtaining products or services. This is a significant improvement on practices that rely on accepting the integrity of documents at face value.

A prototype for the DVS component of the NISS was trialled in 2006. The DVS was redeveloped in response to pilot findings and an OPC privacy audit of the prototype, which concluded that a well-developed DVS "has the potential to significantly reduce the amount of manual interaction with data

[19] More information on the NISS is made available online by AGD, http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity

[20] Australian Bureau of Statistics, *2007-08 Multi-Purpose Household Survey (MPHS)*, Canberra, 27 June 2008, http://www.abs.gov.au/AUSSTATS/abs@.nsf/Latestproducts/3960E810E161F763CA2574740015B7DC?opendocument

[21] Office of the Privacy Commissioner, *Media Release: National privacy survey: ID theft, ID scanning and online privacy concerns are on the rise*, Sydney, 28 August 2007, http://www.privacy.gov.au/materials/types/media/view/6211

in the verification processes thereby minimising privacy risks in relation to data security" and upgraded to the present version in early 2008.[22]

## 7.2 Brief description of the DVS

The DVS enables authorised users to electronically verify, in real time with the agency that issued the identity credential, whether the credential is current (that is not expired, or cancelled), and whether the details appearing on the document "match" those on the agency's database (that is the document has not been falsified or tampered with). The range of documents that can currently be checked via the DVS includes Commonwealth-issued Passports, Certificates of Citizenship and Visas and State issued documents including drivers' licences as well as birth, change-of-name and marriage certificates; the data checked doesn't include photographs or other biometric data.

## 7.3 DVS participants and their roles

The DVS system is reasonably complex. The participants, or elements, and their roles are as follows:

- Individuals – present identifying documents or document details to an organisation in support of their application for a benefit or service. This may be done in person, via online enrolment, phone registration or with an application form.
- User, or relying or querying, Agency – an agency that seeks to verify information provided by an individual as EOI with an Issuer Agency via the DVS Hub and receives a YES/NO/ERROR response to the request.
- Issuer Agencies – a document Issuer agency or nominated agency (NEVDIS) that receives the request to verify the personal information and generates an automatic response via the DVS Hub to confirm or deny whether the details match the database records it holds
- DVS Hub - the component of the DVS infrastructure that connects User and Issuer Agencies and allows for DVS verification requests and responses to be securely routed between them. The DVS Hub does not retrieve any information held by the Issuer Agency, nor does it collect or store any of the personal information transmitted through it.
- DVS Hub Manager – the entity engaged by the DVS Manager to operate the DVS Hub – This is currently the Department of Human Services (which operates the DVS under a Memorandum of Understanding (MoU)). However, the DVS Hub Manager role is not specific to DHS and could potentially be undertaken by another service provider in the future.
- DVS Manager – the custodian of the DVS Hub infrastructure and responsible for coordinating the development, implementation and operation of the DVS. AGD is currently the DVS Manager.

## 7.4 Operating principles

The following operating principles form the basis of the DVS:

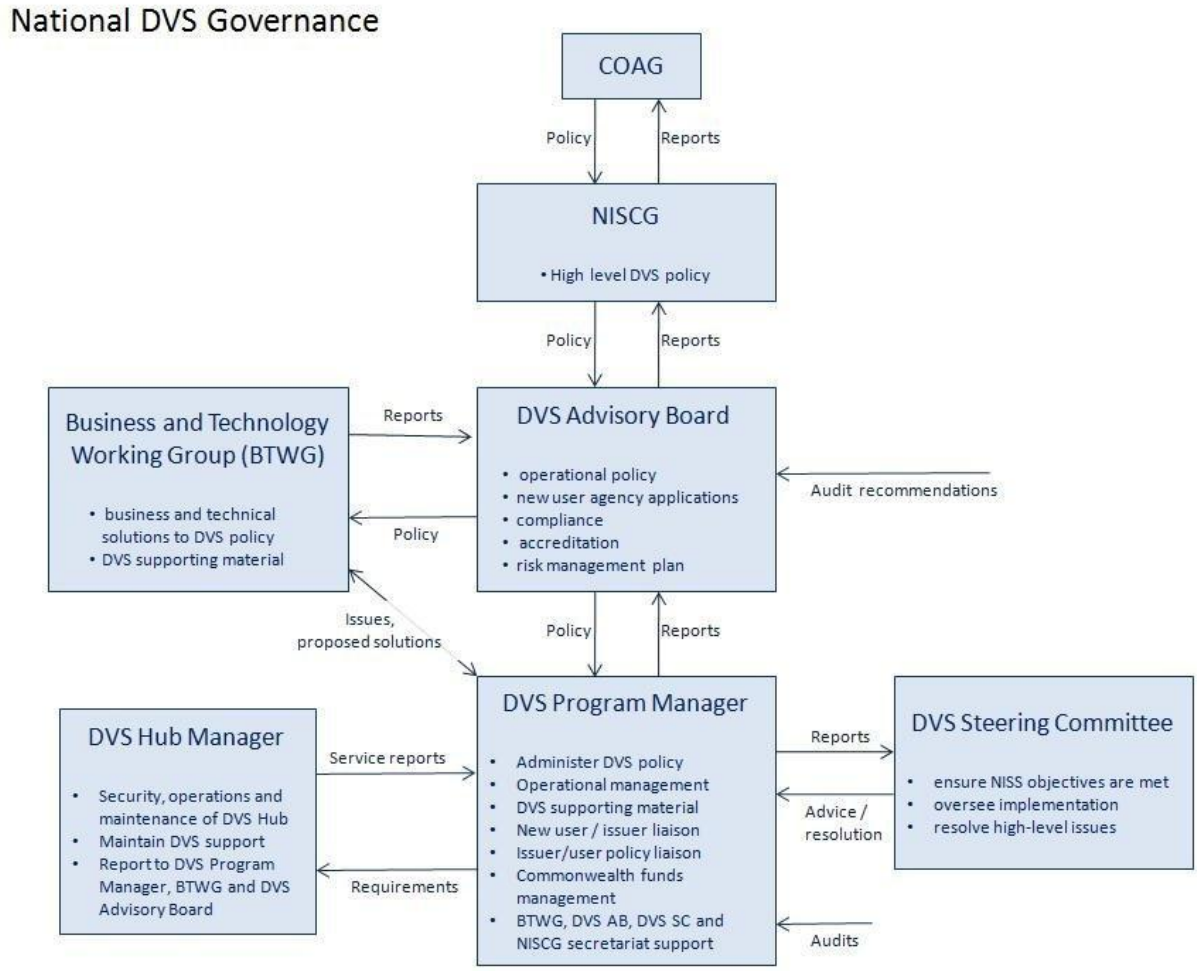
[22] Office of the Privacy Commissioner, '*Document Verification Service Prototype – Final Audit Report*', Sydney, May 2007, http://www.privacy.gov.au/publications/audrep0607.pdf.

- The DVS might replace current verification practices but does not change the way in which Users might handle their customers or otherwise store and manage personal information.
- The DVS provides a means to confirm that the document being presented has identical information to the records held by the document's issuing authority and that the document has not been recorded as cancelled or expired.
- The DVS is a consent-based verification system. Prior to the submission of any personal information from a document presented as EOI informed consent is obtained from the individual presenting the document.
- The function of the DVS is not to store information, but to act as a conduit to verify information that is already collected by user organisations and held by issuing agencies.
- The DVS only matches information from the EOI document with the issuing agency via a YES/NO/ERROR response. It does not retrieve any information held by the issuing agency.
- Information sent to or from the DVS is transmitted using secure, encrypted methods of communication.
- A response received from the DVS must only be used for the purpose of confirming information already contained on an EOI document.
- A querying organisation does not base a decision to grant or refuse an application solely on the basis of a response from the DVS. The DVS does not replace the need for organisations to operate an EOI policy or otherwise exercise due diligence and manage its risks.
- High-level standards and protocols govern the administration, access and use of the DVS.
- The National Identity Security Coordination Group (NISCG) provides high-level oversight and guidance to the development and implementation of the DVS.[23]

[23] The National Identity Security Coordination Group (NISCG) is the primary vehicle for negotiating key elements of the NISS for consideration by COAG. The NISCG includes representation from central agencies of the Australian, State and Territory governments, the Council of Australasian Registrars for Births, Deaths and Marriages, the NSW Registrar for Births, Deaths and Marriages (as lead agency for the Certificate Validation Service), Austroads and the Federal Privacy Commissioner.

## 7.5 GOVERNANCE OF THE DVS SYSTEM

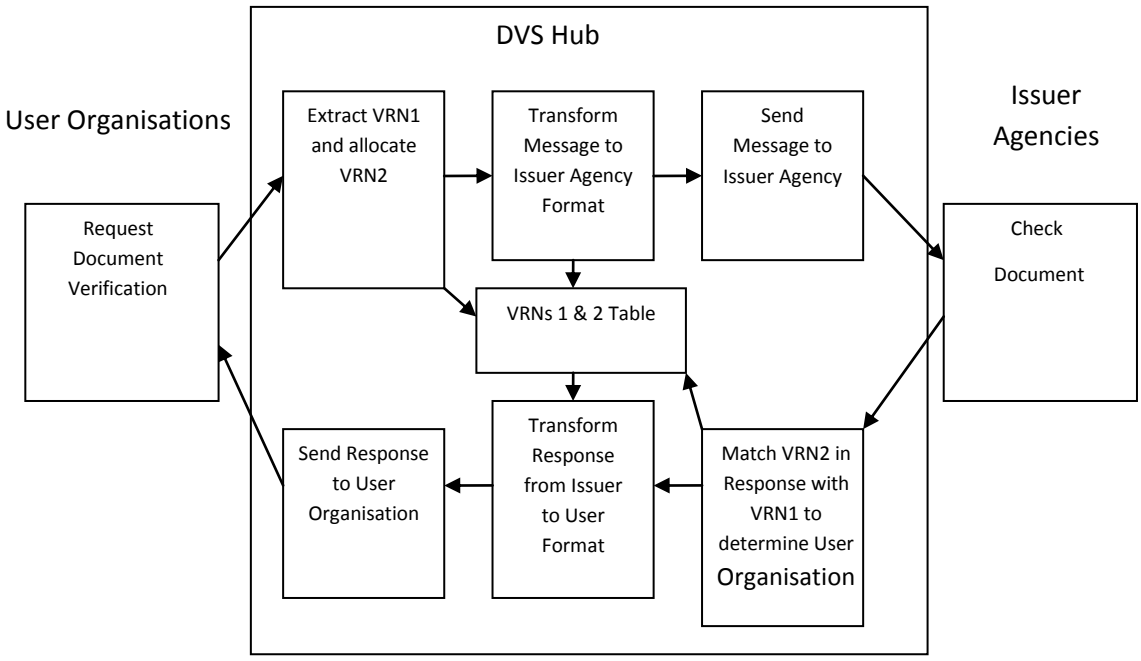
The DVS operates under a formal and well-documented set of governance arrangements that are set out in the diagram below.




## 7.6 DVS – CURRENT SYSTEM PERSONAL INFORMATION FLOWS

This part of the report describes the DVS as it currently operates. The DVS is simply a matching process. Information transfers are facilitated through a DVS Hub but do not involve the retention of any personal information used to conduct the check, nor any linking of information across the participants.

The diagram below sets out the process and it is described in more detail in the sections that follow.




**High-level data process diagram**

As the DVS is a system to match personal identification information from EOI documents, some data transfer of personal information is necessary in the verification process. From a human perspective, the verification process consists of the following steps:

- A person presents their EOI documents; this might be in person, or by phone, an application or online (where the person enters their details, including document details, directly).
- The User Agency gains authorisation from the applicant to undertake checks to confirm details from the documents.
- Details on the identifying document such as name, date of birth, official document registration number (see Appendix 4 for the details which are submitted for verification), or other identifying features are entered into a computer system linked to the DVS.
- The DVS Hub processes the request and sends the information, and in the case of BDM registries, the code for the User agency, via a secure communications pathway to the Issuer Agency where an automated check of the agency's register verifies whether the information provided is matches with information held on the Issuer Agency's database and that the document has not been cancelled.
- If the information provided matches the information held by the Issuer Agency, a YES response is transmitted to the organisation informing them that the document has been

verified; otherwise, a NO response is returned indicating that the document details were not verified. No additional information is divulged or available from the agency's records.

- In normal circumstances a response to the verification request is returned in a matter of seconds.
- It will also be possible that the response to the User Agency is one of two types of ERROR response. The first is a system error, [S], which is returned for system availability issues such as problems with the connection between the agencies and the DVS Hub that cannot be resolved. The second is a [D] for data range error, which occurs when the request pertains to a range of data which has not been electronically captured by the Issuer Agency.
- A new DVS request could then be entered, or the User might consider seeking a secondary manual verification. Secondary verifications are outside the scope of the DVS and will need to be sourced through separate arrangements.
- A User Agency will make decisions about the level of assurance or value it places on the EOI information provided by their customer has submitted for identification purposes taking account of the DVS response as one factor.

As an IT process, the steps are:

- The User Agency submits a query by preparing an electronic message to which it has assigned its own Verification Request Number (VRN1). This is sent as an encrypted package of data from the User's computer system, via secure electronic communications pathways, to an electronic processor (the DVS Hub).
- The DVS Hub gateway confirms that the incoming message has arrived from an authorised source by testing various characteristics of the sender.
- The DVS Hub registers the incoming query using VRN1 and associated other transactional data (metadata) (for example time of the query, electronic notification of the querying party).
- The DVS Hub removes VRN1 and gives the data package a second identifier (VRN2). The DVS Hub records these numbers in a reconciliation table. Where the Issuer Agencies require, the DVS Hub adds the User Agency identifier (Originating Agency Code or OAC), and transfers the query message to the computer system of the relevant document-issuing agency.
- The computer system of the Issuer Agency recognises a transaction as coming from the DVS Hub. It consults the relevant database, establishes if the query data matches the particular data fields, and returns an encrypted "YES", "NO" or "ERROR" response to the DVS Hub, referencing VRN2.
- The DVS Hub receives the response message recording metadata about the receipt and response issued for the transaction.
- The DVS Hub refers to the reconciliation table and establishes a connection between the two VRNs and registers the return of the response.

- The DVS Hub passes on the "YES", "NO" or "ERROR" response to the querying computer system, identified by the first VRN.
- The DVS Hub records the successful transmission of the transaction to the User Agency.

## 7.7 COLLECTION OF PERSONAL INFORMATION

Use of the DVS system presupposes the prior collection and handling of fairly limited personal information (as set out in Appendix 4). The agencies involved will also continue to have obligation to provide notice of the collection of personal information and, in some jurisdictions, their information handling practices generally.

It is also important to note that the DVS is operated on the principle that individuals must first give their consent to have their document details verified.

Users generally implement the DVS in the context of client identification processes they are already undertaking, although some new registration processes are being developed that include a DVS check from the inception. To integrate the DVS into these enrolment processes will not require them to collect any additional information from the individuals concerned than would be required in a non-DVS enrolment process; the service offered by the DVS is to confirm the accuracy of the document information proffered. As a result of the DVS process, the Users will have an indication of whether the EOI information they seek to rely on matches that held by the Issuer Agency.

The DVS Hub is not designed to collect personal information.[24] It receives messages with the personal information content encrypted, undertakes some processing, and passes the information on to the Issuer Agencies. Similarly, it receives information from the Issuer Agencies and passes it to the User Agencies; the Hub does not interrogate the Issuer Agencies databases. The passage of information through the Hub is generally very quick (about 0.2 of a second). While there is an audit log of the transaction, the Hub does not retain any personal information from or about the transactions that pass through it.

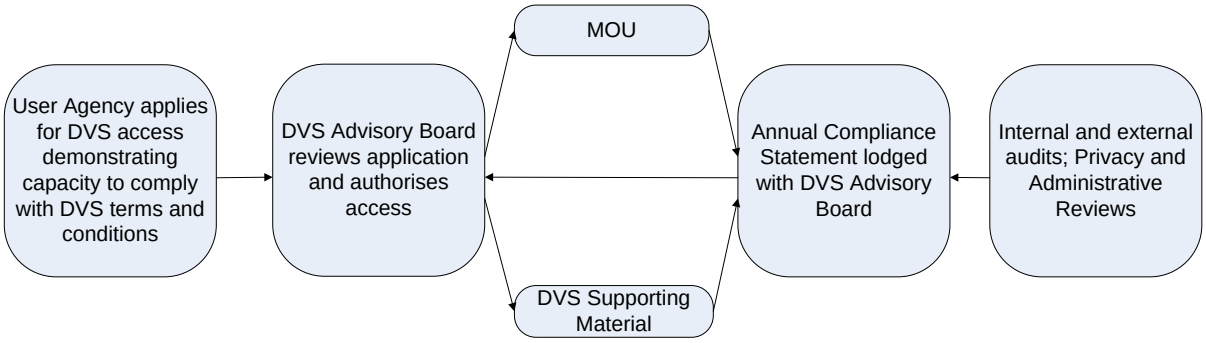
Agencies will already hold the personal information that is to be verified. However, where an Issuer agency receives the OAC code that Issuer will potentially be able to infer that the individual has undertaken a transaction or a series of transactions that require identification. Issuers collecting this information can effectively accumulate a profile their client's activity across other government and business organisations. Currently, OAC codes are provided to Registries of Birth, Deaths and Marriages (eight Issuer agencies in all); the other agencies do not receive this code and would not be aware of the name of the User Organisation making the verification request.

## 7.8 SECURITY

The DVS system is designed for close management of the security of the system. The governance arrangements, new User application processes, contracts, processes to establish technical connections, and information resources and other support material all have a strong emphasis on system and data security.

[24] For a discussion of the DVS design and related personal information flows see the OPC 2007 audit of the DVS pilot available at http://www.privacy.gov.au/materials/types/reports?sortby=29 and the 2007 PIA completed by AGD and available at http://www.ag.gov.au/identitysecurity

All agencies or organisations connecting to the DVS are required to employ IT security processes to ensure that only authorised staff can access the DVS and provide information for a security threat risk assessment on the operation of the DVS. They are also required to report security incidents and to provide an annual compliance statement, which is reviewed by the DVS Advisory Board. The diagram below summarises the check and balances in the system.




Other key features of the DVS security arrangements include that:

- The DVS uses only secure, encrypted methods of communication as a safeguard against unauthorised access to the DVS system.
- The Hub Manager provides a critical role for the effective operation of the DVS in making sure that the system is operating with the specified high level of speed, accuracy and security.
- Information controls are also built into the Hub Manager agreement including a protocol for handling suspected or actual breaches and standards for retention and deletion of personal information.
- A DVS risk assessment and risk management plan feed into the management of the DVS.

## 7.9 ACCURACY

Data accuracy is an important aspect of privacy protection regimes; inaccurate data can impact on the decisions made about individual or cause considerable inconvenience. Maintaining data integrity is also important to achieve the identity security objectives of the DVS. The DVS experience is that by far the main sources of inaccuracy in the EOI checking process flows from data entry mistakes by the User, or the individual when submitting document details. Other sources include:

- attempts to check a document which the Issuer Agency does not hold electronically (for example pre-1974 birth certificates or marriage certificates from Queensland)
- mistakes in the Issuer Agencies databases.

The User and Issuer agencies will be respectively responsible for ensuring that their data collection processes and the personal information they hold is sufficiently "complete, accurate and up-to-date" in the circumstances.[25]

The DVS system design does include features that should minimise the risk to individuals if the verification of their records is affected by poor quality data:

- the personal information used in the DVS is provided by the individual, and in the case of online applications they might themselves enter the details into the system
- the DVS operating principles provide that querying organisations do not base any decision to grant or refuse an application solely on the basis of a response from the DVS, and
- if details from a document are not verified by the DVS, the automatically generated 'NO' response does not disclose the reason for non-verification leaving it open for the User Agency to consider the need for an individual to supply additional identity documentation or information.

## 7.10 Use of personal information

Privacy principles generally require personal information to only be used for the purpose for which it was obtained or related purposes. Personal information transmitted through the DVS is only used to confirm whether the information on the EOI document corresponds to the record held on the document Issuer agency's database. This use supports the identification process and as such, is consistent with the purpose for which the information was collected.

However, as additional protection, the DVS is used only with the consent of the individual concerned, and consent will be sought for the DVS transaction in its entirety.

There will be some permitted secondary uses of DVS transaction information, but not of personal identifying information. For example, DVS transaction records might be used for administrative or billing reasons or to investigate technical problems. For example, where Issuer Agencies are not provided with data on the source of the verification request, they will register the source of transactions as coming from the DVS Hub. Verification that the transaction source is valid is carried out at the Hub to assure Issuer Agencies that all transactions received are from Users authorised by Agreement to use the DVS. Should it be necessary to track the source of a transaction, for example to respond to a freedom of information request or a complaint, this will be done on a case by case basis by the DVS Hub using the VRN reconciliation table.

The DVS has also considered the risks of unauthorised secondary uses by either User or Issuer Agencies. While the risks are considered to be low, the DVS includes measures to discourage unauthorised secondary purposes include:

- the emphasis on informed consent should mean that individuals will be aware of the purpose of the DVS check

[25] As required, for example, in IPP 8, Privacy Act available at http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s14.html

- providing a fast and reliable DVS system, which should mean User Agencies will have less need to create in-house databases of copied of documents whose EOI information has aged in terms of currency and accuracy
- limiting the response message to a YES/NO format that does not disclose the reason/s for non-verification
- stipulation in agreements with DVS Users that information from verification checks is only to be used for purposes for which it was obtained, and
- no storage of personal information in the DVS Hub, apart from exceptional circumstances where an error occurs in transmission of transactions to an issuer agency when a transaction may be held up to 24 hours.

## 7.11 Disclosure of personal information

The various sets of privacy principles take slightly different approaches in setting rules for disclosure; some permit disclosures for the purpose of collection or related purposes, others require the individual to have been advised of the disclosure or for the practice to be so well known the person is likely to be aware of it. All sets of privacy principles provide for exceptions, including where the individual has consented to the disclosure.

As has been noted, the DVS process involves only limited transfers of personal information. The DVS approach of requiring individual consent to DVS verification should, were it needed, authorise any disclosures in the context of the DVS. This would apply to the User Agencies, the DVS Hub and to Issuer Agencies.

The DVS Hub Manager is an agent of the agencies and organisations that are connected to the DVS. Personal information that is contained in a request for verification only needs to be viewed in the rare occurrence of a technical problem with the DVS system. In normal operation, a transaction will be in the DVS Hub for approximately 0.2 of a second. The encryption of personal information in messages sent through the DVS is an additional safeguard against unauthorised disclosure.

It is also important to note that the personal information to be verified with the Issuer Agency is already contained within the records of the Issuer agency. The message information attached to a verification request provides information to a Issuer Agency that an EOI document has been presented for verification.

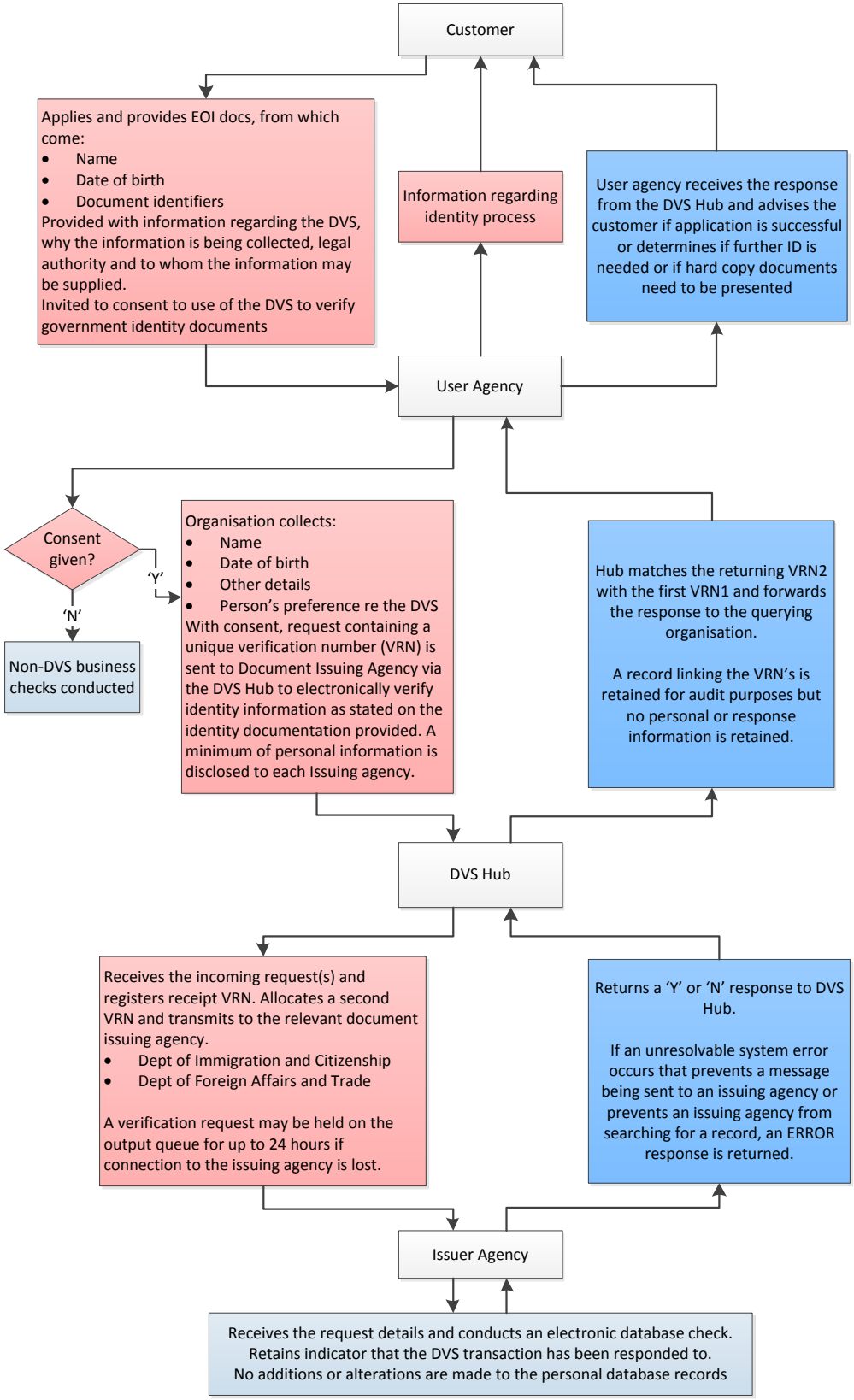
## 7.12 Access and correction

The DVS system will not impact the operation of the relevant access and correction principles. The use of the DVS does not create any new, separate, repositories of information.

The extent to which there may be errors in the details recorded on an identity document or in the electronic records of the Issuer Agency, are matters outside the operation of the DVS. As noted above, the DVS may serve to assist individuals improve the accuracy of data held by Issuer Agencies through “testing” the contents of records. Customers can be advised if their document failed to verify and can seek remedy through the issuer agency if appropriate.

# 8 APPENDIX 3 – DATA FLOWS FOR PRIVATE SECTOR DVS USE

The following diagram sets out the potential information flows should the DVS be utilised by the private sector. It reflects AGD's understanding of the personal information collected, used and retained by the organisations involved.



# 9 APPENDIX 4 – VERIFICATION REQUEST DETAILS

| Document Element | Use in the DVS |
|---|---|
| Birth Date: | Used in all interfaces and can either be in full or partial format. |
| Date Timestamp: | Used in all interfaces to define the date/time at which the request was made as Management Information for the DVS Hub |
| Document Type Code: | Used in all requests to the DVS Hub to define the service that is being called. A document type code can be one of:<br>• Passport (PP)<br>• Driver Licence(DL)<br>• Birth Certificate (BC)<br>• Marriage Certificate (MC)<br>• Change of Name Certificate (CN)<br>• Citizenship Certificate (CC)<br>• Certificate of Registration by Descent (RD)<br>• Visa (VI)<br>• Medicare Card (MD) |
| Family Name: | Used in all interfaces, although the length of the implementing field varies across interfaces |
| Given Name: | Used in all interfaces, although the length of the implementing field varies across interfaces. |
| Middle Name: | Optional |
| Verification Request Number: | Used in all requests to the DVS Hub to uniquely identify the business request. It is passed back to the user in the response message. |
| Originating Agency Code: | Used in all requests to the DVS Hub, a three-character code identifying the organisation and a one-digit number representing the service. |
| Version Number: | Used in all requests to the DVS Hub. |
| Message Id: | Used only by certain agencies for technical purposes. |
| Correlation Id: | Used only by certain agencies for technical identification |

# 10 APPENDIX 5 – DETAILED PRIVACY ISSUES AND RISK ASSESSMENT

The table that follows summarises the key changes in the handling of personal as a result of the extension of the DVS to specified private sector organisations and to allow access by third party agents on behalf of their principal. IIS has made its assessment against the key concepts in the IPPs and NPPS rather than undertaking a detailed assessment against all provisions of the privacy principles applying in all applicable jurisdictions.

| Relevant Privacy Principle | DVS Activity | Private Sector User organisation | Third Party agents<br>Via agencies/organisations IT systems or direct to DVS & working for one or more agencies/organisations | DHS Hub | Issuer Agencies | Impact & Risk assessment |
|---|---|---|---|---|---|---|
| **Collection Anonymity** | The DVS by definition involves EOI document information and cannot function using anonymous or de-identified information. However, the use of encryption technology de-identifies data for anyone not authorised to access the information. The DVS does not allocate an identifier to individuals. | No change | No change | No change | No change | No change |
| **Collection Necessary**<br><br>**Only collect personal information for lawful purposes,** | The DVS is designed to minimise the amount of personal information collected and transferred – only specified, key details (see Appendix 4) entered into the system | No additional information collected as a result of using DVS other than the fact the Issuer agency does or does not verify a | An agent conducting EOI check for an agency or organisation will in the course of that business already collect details from an individual – access to the DVS simply | No change<br><br>DVS Hub used only for DVS purposes, logical separation from any other information, technological severability | About individual – no new information, just what already held<br><br>Where the Issuer agency chooses to collect the OAC identifying the user | Risks – Issuer agencies<br><br>Issuer agencies collecting information about identity of user organisation where not needed for its functions |

| Relevant Privacy Principle | DVS Activity | Private Sector User organisation | Third Party agents<br>Via agencies/organisations IT systems or direct to DVS & working for one or more agencies/organisations | DHS Hub | Issuer Agencies | Impact & Risk assessment |
|---|---|---|---|---|---|---|
| **necessary for functions or activities** | for checking and only yes/no response provided to user organisation<br><br>Individual presents in person or online to organisation or agent with ID documents in the context of an ID check process. Where organisation decides to check validity of ID documents, enters document details and makes request for document matching<br><br>DVS is promoted as a is a consent-based, non-disclosure system | particular document | adds a 'verified' or 'not verified' status to the documents (or document details) tendered. Limited information and necessary in the context. | a requirement. More through put but is not considered to collect personal information so no change – generally, held only long enough to process and pass on (less than a minute to process), content of request encrypted, only decrypted in very rare circumstances where there are technical problems<br><br>(See AGD 2007 PIA and OAIC audits)<br><br>The DVS Hub will collect data on successful completion of DVS transactions for the purposes of billing the user organisation. This will be completed using only the management information recorded at the Hub in relation to the VRNs (i.e. date/time | organisation (BDM Registry Issuer agencies) there is increased collection of information | or activities |

| Relevant Privacy Principle | DVS Activity | Private Sector User organisation | Third Party agents<br>Via agencies/organisations IT systems or direct to DVS & working for one or more agencies/organisations | DHS Hub | Issuer Agencies | Impact & Risk assessment |
|---|---|---|---|---|---|---|
| | | | | stamp). No personal information is retained or recorded. | | |
| **Collection - Privacy notices** | | Private sector organisations subject to the Privacy Act already have obligations under NPP 1.3 to tell people about matters such as purpose of collection and usual disclosures. While the data passed to Issuer agencies already known, it would be good practice to ensure that individuals are explicitly advised about the check with a document's Issuer agency | Agents would have notice obligations, may be covered the in context of agency relationships | No change<br><br>The DVS Hub is not designed to collect personal information other than where necessary on a very short-term basis. Where there are technical or other errors, messages and their data are held until the problem can be fixed. Once resolved the message and any personal information is deleted. | No change<br><br>Federal or State/Territory Issuer agencies generally have obligations under respective privacy laws (eg the Privacy Act, Privacy and Personal Information Protection Act 1998 (NSW)) to take reasonable steps to tell people about matters such as purpose of collection and usual disclosures. Given the nature of the information provided in the course of a DVS check there may be a number of ways to meet reasonable steps including consent process, general information about DVS in privacy policy | Risk:<br><br>Possible compliance risk for user/Issuer agencies and third party agents if notice/consent process not adequate<br><br>If notice obligations not fully met, individuals will not be aware of the nature of the check and what information is transferred to whom<br><br>Risk mitigated if consent process in place and working well. |

| Relevant Privacy Principle | DVS Activity | Private Sector User organisation | Third Party agents<br>Via agencies/organisations IT systems or direct to DVS & working for one or more agencies/organisations | DHS Hub | Issuer Agencies | Impact & Risk assessment |
|---|---|---|---|---|---|---|
| **Collection - Consent** | | Obligation to obtain informed consent is an established condition of DVS use. This could be made clearer as an express requirement of private sector users.<br><br>[DVS private sector application to use DVS T&C of use do not currently specifically mention the need for individual consent – while there is a requirement to comply with all laws etc its important to note the NPPs only require consent to collect or disclose personal information in specified circumstances (sensitive information, unrelated disclosures). The DVS compliance statement does require users to report on privacy matters | Obligation to seek consent as a condition of DVS use might be a new requirement – will need to be clear on whether agency/organisation or agent obtains consent | No Change | No Change<br><br>but noting that if the Issuer agency considers it needs consent to conduct check or provide yes/no response then the consent process will need to be appropriate – informed consent, with sufficient detail about the Issuer agencies' roles | Risks here are:<br><br>• Organisation and/or agent consent practices will be poor (in small print, bundled with other matters where consent is sought, asked after check is conducted, no information provided including about Issuer agencies retaining record of check)<br><br>• Organisations will not actually seek consent if not a specific requirement of Terms and Conditions<br><br>• If consents not being obtained, a risk for the DVS to promote the system |

| Relevant Privacy Principle | DVS Activity | Private Sector User organisation | Third Party agents<br>Via agencies/organisations IT systems or direct to DVS & working for one or more agencies/organisations | DHS Hub | Issuer Agencies | Impact & Risk assessment |
|---|---|---|---|---|---|---|
| | | including consent | | | | as consent based<br>• Without input from individuals (or advocates) consent processes may not be as user friendly as they could be |
| **Collection – Fairness and not intrusive** | | Changes likely to be pro-privacy rather than the reverse<br>Focus of the principle is means of collection - | No changes<br>Focus of principle is means of collection | No change | No changes<br>Focus of principle is means of collection | No specific risks identified |
| **Security** | DVS arrangements have a strong focus on security at all stages in the process – detailed requirements application process, system testing before access to DVS, compliance reporting requirements, monitoring, incident reporting etc | More organisations, different type of organisation accessing the DVS – might introduce new security risks, including possibly increased risk of data security breach | New access arrangement via agents – User organisations agencies have will have obligations to ensure appropriate security in place and an monitored | Information from more/different types of organisations flowing through the Hub, which would need to monitored from a security risk perspective | No change | The move to extend the DVS to private sector organisation may introduce new risks in particular, use of agents that connect direct to DVS, lead agency may not have visibility, will need to rely on DVS reports and proactive oversight of contract |

| Relevant Privacy Principle | DVS Activity | Private Sector User organisation | Third Party agents<br>Via agencies/organisations IT systems or direct to DVS & working for one or more agencies/organisations | DHS Hub | Issuer Agencies | Impact & Risk assessment |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | Risk to individuals if incidents involving personal information are not investigated quickly. | N/A | N/A | N/A | Risks: live data risk may be exacerbated by the expanded system |
| **Openness or Personal Information Digest** | DVS material, MOUs and proposed private sector application T&C require compliance with applicable laws including privacy – no specific material on openness | No change in obligations – good practice to mention use of DVS in privacy policy | New use of DVS – good practice to mention use of DVS in privacy policy | No Change | Privacy regimes in some states call for a privacy policy which describes information handling practices – possibly a need to reflect change in DVS access in the policy | Risk – not clear that there would be compliance issues if DVS not mentioned in PID entries, privacy policies. OAIC audit recommends reference in PID.<br><br>Increasing complexity of the DVS system may make it more difficult for individuals to know/understand who will be handling their document details for what purposes |
| **Access and Correction** | DVS returns no/error messages which could be inaccurate<br><br>DVS material, MOUs and | No change in access/correction obligations | No change in access/correction obligations | N/A | No change in access/correction obligations | No specific risks arising from the DVS system identified |

| Relevant Privacy Principle | DVS Activity | Private Sector User organisation | Third Party agents<br>Via agencies/organisations IT systems or direct to DVS & working for one or more agencies/organisations | DHS Hub | Issuer Agencies | Impact & Risk assessment |
|---|---|---|---|---|---|---|
| | proposed private sector application T&C require compliance with applicable laws including privacy – no specific material on access and correction | | | | | |
| **Accuracy** | Submitting a document for matching<br><br>Data entry errors a major reason for a "no" response<br><br>DVS has steps in place to improve accuracy of data entry, avoid submission of no electronic documents. | Individual may present to organisation (or their agent) that will enter data into the DVS interface or use online service where Individuals enter data themselves<br><br>Request for verification submitted If the result is No or error, organisation will tend to ask for another document to check, rather than necessarily checking if the problem its own data entry, or if in fact its not possible for document to be checked (eg older birth certificates or marriage certificates in | Agents/user agencies would need to take reasonable steps to ensure systems/processes promote accuracy | No change | No change - steps to support individuals to become aware of and correct any document accuracy problems would presumably be supported | Risk: Individual won't know if the 'No' response is a data entry error, a non-electronic document or a problem with their identity document and so may waste time in trying to get problem fixed. Individual may be disadvantaged, particularly if they have only a few of the possible documents that could be verified |

| Relevant Privacy Principle | DVS Activity | Private Sector User organisation | Third Party agents<br>Via agencies/organisations IT systems or direct to DVS & working for one or more agencies/organisations | DHS Hub | Issuer Agencies | Impact & Risk assessment |
|---|---|---|---|---|---|---|
| | | some states) DVS check is not a requirement of businesses but an option. Introduction of DVS into process does not, of itself, result in this problem. | | | | |
| **Use, Relevance and Function creep** | Limiting the response message to a YES/NO format that does not disclose the reason/s for non-verification (other then error messages)<br><br>Stipulation in Agreements with DVS users that information from verification checks is only to be used for purposes that were the subject of consent by the individual concerned, | Private sector organisation not obtaining new information other than that the EOI documents have or have not been verified<br><br>Possible that the fact that an individual's EOI documents have been verified adds to the value in potential re-use of the customer information but noting that this should be proscribed by the contract. | Agent not obtaining new information other than that the EOI documents have or have not been verified<br><br>Possible that the fact that an individual's EOI documents have been verified adds to the value in potential re-use of the customer information but noting that this should be proscribed by the contract. | No change<br><br>No storage of personal information in the DVS Hub, apart from exceptional circumstances where an error occurs in transmission of transactions to an issuer agency when a transaction may be held up to 24 hours. | Where the Issuer agency chooses to collect the identity of the user organisation (BDM Registry Issuer agencies) increased collection of information | Risk: if Issuer agencies seek to know the identity of the agency/organisation requesting verification and retains this information, will be increasing richness of data trail about individuals' interactions with government and private sector - potential for use for new purposes, exacerbated longer the information is kept<br><br>OAIC – similar finding and recommends MOU specific limitation in re- |

| Relevant Privacy Principle | DVS Activity | Private Sector User organisation | Third Party agents<br>Via agencies/organisations IT systems or direct to DVS & working for one or more agencies/organisations | DHS Hub | Issuer Agencies | Impact & Risk assessment |
|---|---|---|---|---|---|---|
| | | | | | | use |
| **Disclosure** | DVS processes request<br><br>The data package which constitutes the response does not contain personal information so no disclosure by Issuer agencies | Only transfers information about the document that is already known to the Issuer organisation<br><br>On-selling of identified customer lists – this should be proscribed by the contract, Possible that the fact that an individual's EOI documents have been verified adds to the value in potential disclosure/sale of the customer information | Similarly, possible that the fact that an individual's EOI documents have been verified adds to the value in potential to on-sell (disclose) their information | | Issuers only see details that they have already issued and only provide Yes/No responses | Risk that third party agents will on-sell or reuse customer information that is known to be more accurate as documents are verified but contract/oversight arrangements should minimise this risk. |
| **Limits on use of Commonwealth or State unique identifiers** | | NPP 7 issues but ok in context of legal obligations to undertake client identification | NPP 7 but ok in the context of agency/principal relationship | No new issues | No new issues | No issues |
| **Transborder data flows** | As far as known no transfer of information outside Australia | No change<br><br>No specific restriction in MOU or contract | No change<br><br>No specific restriction in MOU or contract | No change | No change as a result of private sector extension | No issues for the DVS |

| Relevant Privacy Principle | DVS Activity | Private Sector User organisation | Third Party agents<br>Via agencies/organisations IT systems or direct to DVS & working for one or more agencies/organisations | DHS Hub | Issuer Agencies | Impact & Risk assessment |
|---|---|---|---|---|---|---|
| **Governance** | Rigorous and well documented governance process, with clear roles, responsibities, documentation, monitoring, some independent auditing | Private sector organisations not subject to audit by the OAIC but will be subject to audit by independent auditors | Business segregation measures are required of Agent to ensure that the DVS is used only to verify clients of authorised DVS User agencies | No change | No change | Risks – Governance process not tailored to private sector organisations and so overlooks aspects of governances. Low risk given strength of process but risk increases if resources not available to continue rigorous regime, risks also increases with introduction of agents or if no appropriate audit |
| **Safety Net** | In general the DVS expects Issuer agencies and user/agencies to deal with complaints from individuals about their part of the system. Will take a role if appropriate<br><br>Should it be necessary to track the source of a transaction, for example to respond to a freedom of information request or a complaint, this will be | Some private sector user organisations, if small business operators, may not be subject to the Privacy Act. However, IIS understands that it DVS access would be subject to Privacy Act coverage.<br><br>If no Privacy Act coverage, implications for customer if document rejected | Involvement of agents makes the system more difficult for a customer to understand, or have problems resolved | No change | Possibly a change in the volume of requests and therefore the numbers of errors that need to be resolved | Risk - While not a change if user organisations are not subject to the Privacy Act, individuals may have less redress if things go wrong, particularly with notice or security<br><br>Involvement of third party agents makes the system more difficult to |

| Relevant Privacy Principle | DVS Activity | Private Sector User organisation | Third Party agents<br>Via agencies/organisations IT systems or direct to DVS & working for one or more agencies/organisations | DHS Hub | Issuer Agencies | Impact & Risk assessment |
|---|---|---|---|---|---|---|
| | done on a case by case basis by the DVS Hub using the VRN conversion table. | If a verification returns a false negative, agreed there will to be a process whereby the holder of the documents can correct information in the issuer's records (consistent with privacy principles)<br><br>Wrong rejection and no other docs available – As above for wrong rejection; | | | | understand or navigate |
| **Identity management system as a whole** | Limited choice on which ID doc to use | Increasing use of DVS, other options for ID verification reduced | Increasing use of DVS, other options for ID verification reduced | | No change | Low risk as DVS considers a range of docs and is looking to add more but needs to be considered – Possible risk for people who don't have any of the ID docs which are able to be verified via the DVS |