Australian Government

Attorney-General's Department

Privacy Impact Assessment

National Document Verification Service

June 2007

Privacy Impact Assessment

National Document Verification Service

1 Introduction

Identity security is an issue of critical concern to Australian citizens, government and business. It is essential to Australia's security and economic wellbeing that the identities of people seeking access to government or commercial services, benefits, official documents and positions of trust, can be accurately verified in order to prevent the use of false identities.[1] Identity theft is also a major invasion of privacy and a high level concern in the Australian community.[2]

The National Document Verification Service (DVS) is being developed as part of the National Identity Security Strategy which includes a range of initiatives to strengthen national arrangements at each point along the identity security continuum to improve the security features of identity documents, provide premium standards for enrolment and authentication processes, and consider ways to improve the integrity of identity data holdings and the means by which nationally interoperable biometric security measures could be adopted.

Improving procedures for verifying the integrity of key identity documents is a central component of the National Identity Security Strategy. The DVS will enable authorised user agencies to electronically verify, in real time, the detail on key proof of identity (POI) documents which clients provide when registering or enrolling for benefits or services, or possibly as part of an application to receive an 'identity' document. It is intended that the DVS be used by all Commonwealth, State and Territory agencies delivering high value benefits or services to strengthen and enhance existing proof of identity processes and systems. This represents not only a way to improve identity security, but also to promote privacy protection.

The DVS is essentially a means for verification of personal identity information and as a national initiative will be a project of significant scope. Therefore it is appropriate to undertake an assessment of the privacy impacts of the DVS. This Privacy Impact Assessment has been developed with reference to the *Privacy Impact Assessment Guide* released by the Australian Government's Office of the Privacy Commissioner (OPC) in August 2006 and the OPC's Audit Report of the Document Verification Service Prototype.

This document will inform the development of the DVS which is currently underway and is intended to operate as a living document. Further assessment of privacy impacts will be considered if the planned operation and parameters of the DVS change materially from those described in this document.

[1] Council of Australian Governments Special Meeting on Counter-Terrorism, *Communiqué*, 27 September 2005 (http://www.coag.gov.au/meetings/270905/index.htm#Identity)

[2] Address by Karen Curtis, Privacy Commissioner at the Safeguarding Australia Conference, Canberra 12-14 July 2005 at http://www.privacy.gov.au/news/speeches/sp06_05.pdf (7 December 2006)

2 Background

The genesis of the DVS lies in a "Feasibility Study for a Document Verification Service" jointly conducted in 2003 by relevant Australian Government and State and Territory government agencies. The study found that POI processes could be significantly strengthened and registrations/enrolment of persons for high value transactions made less open to fraud if agencies were able to confirm the personal information appearing on key POI documents. It recommended that a DVS should be implemented in a measured and staged manner taking account of key agencies' ability to incorporate the necessary functionality with their existing business and information technology systems.

The issue of identity security was addressed by the Council of Australian Governments (COAG) Special Meeting on Counter-Terrorism 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 heads of government agreed to the development and implementation of a National Identity Security Strategy to better protect the identities of Australians.

As a result of the COAG decision the National Identity Security Coordination Group (NISCG) was established to coordinate the development and implementation of the national strategy. The NISCG is the primary vehicle for negotiating key elements of the National Identity Security Strategy for consideration by COAG.

A prototype DVS (the prototype) was trialled from February to June 2006, to explore the technical and operational issues associated with implementing and running a document verification service to government agencies. The prototype was limited to the Department of Foreign Affairs and Trade and the Department of Immigration and Multicultural Affairs checking POI documents offered by individuals seeking Australian passports and citizenship certificates.[3] The prototype was used to process over 51,000 requests to check the details appearing on birth certificates, citizenship certificates, driver's licences and passports.

An evaluation of the prototype demonstrated its technical feasibility; that secure connectivity has been achieved using dedicated lines; and that verification of the data is viable in an online environment. The findings from the evaluation are assisting with the design, cost and build of the full scale DVS and complement other work being undertaken on the development of the National Identity Security Strategy.

A privacy audit of the prototype concluded that personal information handled in respect of the DVS was well managed in accordance with the Information Privacy Principles in the *Privacy Act* and that a well developed DVS "has the potential to significantly reduce the amount of manual interaction with data in the verification processes thereby minimising privacy risks in relation to data security".[4]

[3] Proof of Identity documentation checked was restricted to Passports, Citizenship certificates and ACT/NSW Birth Certificates and Driver's Licenses.

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

3 National Document Verification Service Project Description

3.1 Vision

The DVS is pivotal to the introduction of more rigorous and accurate national identity security measures. In particular it will strengthen and support client enrolment and registration processes by providing government agencies with greater certainty of the identity of prospective clients.

3.2 Objective

The DVS will enhance the integrity of agencies' POI procedures by providing an assurance that a person is establishing eligibility with verifiable documents. It is envisaged that the DVS will become an accepted and integral part of an agency's POI procedures by minimising:

- the registration and subsequent use of false identities, and
- the occurrence of multiple enrolments for fraudulent purposes.

The DVS will enable authorised user agencies to verify the detail on key Australian POI documents which clients provide when registering or enrolling for benefits or services, and possibly as part of an application to receive an identity document.

When integrated into government enrolment processes, use of the DVS will allow agencies to:

- replace the need for cumbersome and expensive manual processes that allow only a small fraction of applications to be verified
- conduct more checks on key POI documents during enrolment, providing greater confidence in the identity of those to whom services are provided
- integrate the verification response into their enrolment and business processes to gain further efficiencies
- verify POI documents issued by agencies in a different jurisdiction, and
- avoid the need for separate negotiations for access with a variety of document issuing authorities.

3.3 What is the DVS?

The DVS will be a secure, national, real time, on-line system which allows authorised Commonwealth, State and Territory Government agencies to verify the details of documents presented to them as POI with the data recorded in the register of corresponding document issuing agencies.

Verification requests and responses will be facilitated by a DVS Hub which will direct responses and requests to appropriate agencies. All communication through the Hub will be encrypted.

It is intended that the DVS allow participating agencies to verify that:

- a document was in fact issued by the document issuing agency claimed on its face
- the details recorded on the document correspond to those held in the document issuing agency's register
- the document is still valid (ie has not been cancelled or superseded), and
- the document has not been lost or stolen.

3.4 Operating principles

The following operating principles will form the basis for the DVS.

- The DVS will replace current verification practices but will not change the way in which agencies deal with personal information
- Document issuing agencies will maintain ownership and control of their data and systems
- The DVS will provide a means of verifying that the document being checked has identical information to the document originally issued
- The DVS will only seek to verify information from the POI document with the issuing agency. It will not retrieve any other information held by the issuing agency
- The function of the DVS is not to store information, but to act as a conduit for the verification of information that is already held by issuing agencies
- Information sent to or from the DVS will be transmitted using secure, encrypted methods of communication
- A querying agency will not base a decision to grant or refuse enrolment for a benefit or service solely on the basis of a response from the DVS
- A response received from the DVS will only be used for the purpose of verifying information included on a POI document
- Standards and protocols will govern the administration, access to and use of the DVS
- The National Identity Security Coordination Group will provide high level oversight and guidance to the development and implementation of the DVS.[5]

[5] The National Identity Security Coordination Group is the primary vehicle for negotiating key elements of the National Identity Security Strategy 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.

4 Current Verification Processes

Currently government agencies require applicants for high value identity documents to provide POI documents in support of their application. Application forms commonly indicate that the agency receiving the application may seek to verify POI documents with relevant document issuing agencies.

The information from POI documents is copied and retained either electronically or on a paper file. Where it is deemed appropriate, verification of POI documents is undertaken manually or in some cases through on-line subscription to the document issuing agency's database.

Manual verification involves forwarding personal information to the document issuing agency by mail, fax or transcribing it over the phone. If this occurs the document issuing agency will undertake a manual search of their registers and usually respond with a copy of the document or additional supporting detail about the applicant.

Current on-line verification services include:

- the Certificate Validation Service (CVS) provided by the Council of Australasian Registrars of Births, Deaths and Marriages.
- The National Exchange of Vehicle and Driver Information System (NEVDIS) operated by Austroads on behalf of most state and territory road traffic and transport authorities.

5 Mapping DVS Information Flows

5.1 Information flows

The DVS is essentially a system to verify personal identification information from POI documents. Therefore it will necessarily involve some data transfer of personal information in the verification process.

As noted above, the DVS will not change the way in which agencies deal with personal information. Rather it will provide a way to replace current manual practices and link a comprehensive range of documents and create a single online verification mechanism.

From a human perspective, it is intended that the verification process consist of the following steps:

- A person presents their POI documents to an agency in support of their application for a benefit or service.
- The agency (querying agency) seeks authorisation from the person to undertake checks to verify the documents.
- Details on the identifying document such as name, date of birth, official registration number of the document, or other identifying features are entered into a computer system linked to the DVS.
- The information is sent via a secure communications pathway to the document issuing agency where an automated check of the agency's register will verify

whether the information provided is identical to the information on the document.

- If the information provided matches the information held by the issuing agency, a YES response is transmitted to the querying agency informing them that the document has been verified; otherwise, a NO response is returned indicating that the document details were not verified.
- In normal circumstances a response to the verification request will be returned in a couple of seconds.
- If there is a system error, such as problems with connection between the agencies and the Hub, which cannot be resolved an ERROR response will be generated. The new DVS request could be entered or manual verification sought.

As an IT process, the steps will be:

- the verification check, or query, will form an electronic message sent as an encrypted package of data from the querying agency's computer system, via secure electronic communications pathways, to an electronic intermediary/processor called the DVS Hub.
- the DVS Hub will register the incoming query by assigning a virtual reference number (VRN) and associated certain other transactional data (metadata) with that VRN (eg time of the query, electronic notification of the querying party).
- the DVS Hub will give the data package a second VRN, for the use of the document issuing agency, and refer the query to the computer system of the relevant document issuing agency.[6]
- the computer system of the document issuing agency will consult the relevant database, established if the query matched the particular data fields, and return an encrypted "YES", "NO" or "ERROR" response to the DVS Hub, that communication was identified with the second VRN.
- the DVS Hub will establish a connection between the two VRNs.
- the DVS Hub will communicate the "YES", "NO" or "ERROR" response to the querying agency's computer system, identified by the first VRN.

The diagram at Attachment A depicts these steps. A table setting out the details from POI documents to be verified is at Attachment B.

Therefore there are three parties to the information flow for each verification process:

1. the querying agency which sends personal information details from the POI document to be verified and receives a YES/NO/ERROR response to the request,
2. the document issuing agency which receives the request to verify the personal information and generates a response to confirm or deny whether the details match the database records it holds, and

[6] The VRN sent to the document issuing agency will include information about which agency sent the request.

3. the DVS Hub Manager which facilitates the operation of the hub to direct requests to document issuing agencies and responses from the document issuing agency to the querying agency.

The DVS Hub is currently being operated by Centrelink under a Memorandum of Understanding (MOU). However, the DVS Hub manager role is not specific to Centrelink and could potentially be undertaken by another service provider in the future. The MOU for the DVS Hub Manager includes obligations to ensure that Information Privacy Principles (IPPs) are adhered to and that the DVS will maintain a high level of responsiveness to requests.

The DVS is just a verification process. Information transfers will be facilitated through a DVS Hub but will not involve the retention of any personal information used to conduct the verification nor any linking of information across agencies.

Only government agencies will be able to use the DVS at this time. Agencies will only be able to use the DVS for high value benefits and services and will need to be approved. Approved agencies will enter into Memoranda of Understanding with the AGD setting out the arrangements for access and use of the DVS.

The Australian Crime Commission (ACC) is developing a Lost and Stolen Document Register (LSDR) to enhance the accuracy of DVS verifications. The ACC would have no role in using the DVS for enrolment / registration purposes. It would merely provide an aggregated source of information about documents reported as lost or stolen. Details of how this will link to the DVS are still being determined. Further consideration of the privacy impact of the LSDR will be given in determining how this information will be linked to the DVS.

5.2 Collection

DVS querying agencies will make use of information from key POI documents already being collected as part of their normal procedures for registration and enrolment for POI documents and government services. These agencies' registration and enrolment procedures will include advice to applicants that information provided in relation to the application will be checked with relevant sources to verify its accuracy and seek their consent to this.

The details to be entered into the DVS as a query (as detailed at Attachment B) are considered to be the minimum amount of data necessary for the validation of the specific POI document.

Most verification transactions will occur instantaneously and will be encrypted.

However, the DVS Hub will need to be able to retain a DVS message containing personal information if the connection to, or computer system of, a user agency is not operating. The DVS Hub will include a 'persistent messaging' function allowing the system to regularly retry a connection to the appropriate agency. This function is necessary to avoid the requirement for staff to repeat DVS requests.

It will be possible for the DVS Hub to retain an undelivered message for up to 24 hours. If the message is still undelivered by this time an error message will be returned. Therefore it will be possible for the DVS Hub to hold a verification message for up to 48 hours if there is a fault at both stages between the querying agency and the DVS and the DVS and the document issuing agency. However the personal information in the requesting message will be deleted after no more than 24 hours or when the message was successfully delivered to the document issuing agency. The response to the querying agency will only contain a virtual reference number and the issuing agency’s YES/NO response.

The Hub Manager will not retain any personal information once the verification process is completed, just a log of transactions containing verification reference numbers and necessary audit information. The audit information will include Virtual Reference Number(s), requesting agency, document type, verification response (including any error code), and date-time stamps.

5.3 Use

Personal information transmitted through the DVS will only be used to confirm whether the information on the POI document corresponds to the record held on the document issuing agency’s database.

This use supports the enrolment/registration process and as such is consistent with the purpose for which the information was collected.

Use of the DVS will only occur with the consent of the individual concerned. Consent obtained by the querying agency will amount to consent for the DVS transaction in its entirety. For the querying agency that obtains the individuals’ consent to verify documentation provided, consent will be express. Responding agencies and the Hub Manager will not practically be able to obtain their own consent but can imply consent from the requirement that the querying agency obtain consent to the transaction as a whole.

The proposed DVS operating principles also provide that querying agencies will not base any decision to grant or refuse enrolment for a benefit or service solely on the basis of a response from the DVS. If details from a document are not verified by the DVS, the automatically generated NO response does not disclose the reason for non-verification and may require further consideration by the querying agency. This will be a matter for requesting agencies to determine as part of their registration and enrolment processes.

Measures to be in place to prevent use for secondary purposes include:

- limiting the response message to a YES/NO format without disclosing the reasons for non-verification, and
- stipulation in the MOUs with DVS user agencies that information from verification checks will only be used for purposes consented to by the individual concerned.

Linking of data through the DVS will be limited to matching the details from a hard copy document with the electronic records of the document issuing agency. The Hub Manager will not store any of this information beyond the transfer of the request and response.

5.4 Disclosure

The sending of the personal information in a verification request or response to the DVS Hub does not amount to disclosure. The DVS Hub Manager is an agent of the agencies which are connected to the DVS. The encryption of personal information in messages sent through the DVS is a safeguard against unauthorised disclosure. As an agent of the agencies connected to the DVS, the DVS Hub manager would only need to view the data, if at all, to correct a technical problem with the DVS system.

The personal information sought to be verified with the issuing agency is already contained within the records of the issuing agency. Therefore while an information transfer will take place it will not be disclosed to the issuing agency. The VRN information attached to a verification request provide information to a document issuing agency that a POI document has been presented for verification and which agency is seeking verification and may amount to disclosure.

The verification response sent from the document issuing agency is not a disclosure as it is merely a YES / NO response and of itself does not constitute personal information.

It is also significant that these information transfers will only occur with the consent of the person to whom the personal information relates.

The consent to verification obtained by the querying agency will cover the possibility of investigation by the DVS Hub Manager as part of the verification process.

5.5 Access and correction

The personal information obtained by the querying agency and used for the DVS process is that which is on the POI document provided by individuals seeking registration or enrolment for benefits or services. There is no issue about access to this information or correction as it is provided by the person to whom it relates.

To the extent that there may be errors on the document or electronic records of the document issuing agency is a matter outside the operation of the DVS.

5.6 Security Safeguards

All agencies connecting to the DVS will be required to employ IT security processes to ensure that only authorised staff can access the DVS and to provide information for a security threat risk assessment on the operation of the DVS. These processes will inform and support the development of a DVS risk management strategy.

All information sent to or from the DVS will be transmitted using secure, encrypted methods of communication as a safeguard against unauthorised access to the DVS system.

The Hub Manager will provide a critical role for the effective operation of the DVS in making sure that the system is operating with the high level of speed and accuracy required. The Hub Manager will need to be able to decrypt messages to investigate errors or system failures should they arise but would not do so routinely.

Safeguards will also exist in relation to the Hub Manager's access to information. Logistical and practical barriers to prevent inappropriate staff access to personal information through the DVS will include:

- Access to systems associated with the Hub being restricted to a small number of IT staff,
- Access to the IT system being based on a secure logon and a further logon and password to access the Hub systems,
- The absence of a general user interface for IT staff to retrieve and review DVS messages, and
- Personal information transmitted through the Hub will not be retained for longer than 24 hours
- An audit log of information transfers and investigation of particular transactions by the Hub Manager will be retained and available to be reviewed.

The Agreement with the Hub Manager will include a requirement for deletion of message information. In most cases where there is no error this will occur instantly. If investigation is required the personal information will be deleted after no more than 24 hours.

Information controls will also be built into the Hub Manager agreement including a protocol for handling suspected or actual breaches, minimum standards for retention and deletion of personal information. A DVS risk assessment and management plan will also be developed as part of the DVS project development and will feed into the design of the DVS.

5.7 Data quality

In developing the DVS it is intended to enhance data quality to support the DVS by negotiating for the back capture of data on key POI document databases. This will also be complemented by measures to improve data integrity being developed as part of the National Identity Security Strategy.

While data integrity is important for the achievement of the identity security aims of the DVS, the impact of inaccurate personal information on individuals is minimised by the design of the system in several ways:

- The personal information used in the DVS is provided by the individual,
- The proposed DVS operating principles also provide that querying agencies will not base any decision to grant or refuse enrolment for a benefit or service solely on the basis of a response from the DVS,
- If details from a document are not verified by the DVS, the automatically generated NO response does not disclose the reason for non-verification and may require further consideration by the querying agency.

Any non-verifications due to a discrepancy between the POI document and the database held by the document issuing agency will not be caused by the DVS but the verification process may be a trigger for this to be resolved. It is the responsibility of document issuing agencies to ensure that their databases are accurate and up-to-date. In fact the DVS helps to improve the data quality of personal information held by government agencies by providing another mechanism to substantiate the accuracy and currency of personal information collected by these agencies.

5.8 Identity management system

The DVS by definition involves POI document information. There is no scope for the DVS to proceed through the handling of completely anonymous or de-identified information. However, the use of encryption technology will de-identify data for anyone not authorised to access the information. The DVS will not result in the allocation of an identification number to individuals.

The DVS will not authenticate the identity of persons; just verify the validity of POI documents. Other measures dealing with linking the person to the POI document and preventing forged documents are being considered as part of the National Identity Security Strategy but are beyond the scope of the DVS.

6 Privacy Impact Analysis

The DVS is still in the design stage and this privacy impact assessment is being undertaken as part of the Australian Government's commitment to ensure that privacy considerations are reflected in the development and implementation of the DVS. The funding arrangements for the DVS reflect this commitment, providing funding for the OPC to assist in this task.

The collection of personal information from POI documents occurs as part of existing registration and enrolment processes. The DVS process will just provide an automated mechanism for verifying this information.

While the DVS will provide scope to process a much larger number of verification requests, the amount of personal information about an individual will be limited. Aggregation of information is not a significant risk of the DVS because of its design features such as encryption and limited retention of personal information in the Hub.

The role of the DVS Hub Manager has been given careful consideration. This is a new risk introduced by the DVS in comparison to existing verification processes because it introduces a new system and party to verification processes. This needs to be weighed against factors which reduce risk.

Centrelink will be the Hub Manager and is developing the DVS Hub under agreement with the Attorney-General's Department (AGD). To the extent that Centrelink is an agent for AGD, it acts subject to AGD's obligations under the IPPs. As a Commonwealth agency Centrelink is also subject to the *Privacy Act 1988* (Cth) in its own right. Handling personal information (including much that with a much greater level of sensitivity than will be processed through the DVS) is Centrelink's core business. The design of the DVS does not require that Centrelink would have to remain the Hub Manager. However, any consideration of a different Hub Manager in the future should consider the robustness of the information privacy handling credentials of the organisation and maintain the requirement that IPPs in the *Privacy Act 1988* (Cth) are complied with.

The security safeguards (as described above) are a significant mitigation of any risk of inappropriate breaches of personal privacy through the DVS Hub.

Automation reduces the number of people involved in verifying a person's POI documents. There is no need for an employee of a document issuing agency to see the verification request and related personal information, the verification is undertaken automatically by the computer application. Consequently there is less risk of, and opportunity for, a privacy breach occurring as the only people exposed to the information are the limited number of processing staff within querying agencies.

The automation allows further controls such as encryption and the generation of an audit log to be applied to the process to better protect the information flows and reduce the level of exposure of personal information.

The fact that the DVS verification will only be undertaken with the consent of the person providing the POI document is also significant. Information will be available about the purpose of verification and flow of information through the DVS Hub to the document issuing agency and corresponding response message.

Citizens' trust in government is critically affected by the standard of its information handling. Appropriately designed, the DVS will enhance accurate confirmation of an individual's identity, reducing the likelihood of identity theft and providing reassurance that governments can carry out their functions efficiently while respecting personal privacy.

By automating the current processes for verifying POI documents and including security safeguards and controls, the DVS could be generally more privacy enhancing than alternative manual practices. Individuals will also benefit from the increased speed of approval of benefits and services, through a more robust and faster enrolment process. An individual applicant can also have greater confidence in the security of their information as it is being processed.

Strong project development planning including:

- risk assessment and review,
- governance arrangements, and
- standards and protocols to govern DVS administration, access and use

will support the above measures to appropriately manage the privacy impact of the DVS. This is being progressed as part of the development of the DVS and proposed actions are further discussed in the Privacy Management section below.

This PIA has been developed to look at the compliance of the DVS with the *Privacy Act 1988* (Cth). DVS user agencies are affected by a range of legislative requirements – both federally and in States and Territories. Participating States and Territories are encouraged to consider the impact of the DVS within their jurisdictions. The OPC will also undertake further analysis of cross-jurisdictional privacy regulation as required.

7 Compliance with IPPs

In addition to the privacy impacts described above, an assessment has been made of how the DVS will operate in accord with the IPPs applicable to Commonwealth agencies under the *Privacy Act 1988* (Cth).

IPP 1 – Manner and purpose of collection of personal information

- The DVS makes use of personal information already being collected by querying agencies and document issuing agencies. The verification of this information by querying agencies is directly related to the purpose for collecting the POI document – confirming a person's identity information.
- Any collection by the Hub Manager is temporary and for a legitimate purpose of IT service provision under agreement with the Attorney-General's Department. To the extent that the Hub Manager receives personal information it will only be to facilitate its role as an agent for DVS user agencies in the transmission of verification requests and responses.

IPP 2 – Solicitation of personal information from the individual concerned

- Personal information entered into the DVS will be solicited by the querying agency as part of its existing registration or enrolment process. These agencies inform individuals why the information is being collected, the legal authority to do so and who the information is usually supplied to.
- DVS verification will be undertaken with the consent of the individual concerned.
- Commonwealth agencies participating in the DVS are already subject to IPP requirements and the DVS will not change their IPP 2 obligations.
- The Hub Manager role does not involve the solicitation of additional personal information. Any collection of personal information by the Hub Manager is temporary and for a legitimate purpose of IT service provision under agreement with the Attorney-General's Department.

IPP 3 – Nature and method of personal information solicited

- Only personal information relevant to confirming the validity of a POI document will be verified.
- The DVS is a mechanism for agencies soliciting the POI information to ensure that it is up to date and complete.
- The collection of the information will not unreasonably intrude on the individual as it will be based on informed consent as part of a wider enrolment or registration process.

IPP 4 – Storage and security of personal information

- Secure communication lines and encryption of the information being transmitted will provide technical security to protect against unauthorised access, use or disclosure of personal information transmitted through the DVS.
- Centrelink as Hub Manager will comply with IPP 4 using such means as are necessary including appropriate logistical and practical barriers to prevent inappropriate staff access to personal information.
- MOUs with DVS user agencies and the Hub Manager will include provisions requiring compliance with IPP 4.

IPP 5 – Information relating to records kept by record-keeper

- The DVS Hub will facilitate an information transfer but will not retain any personal information which is disclosed to it through the Hub. Any possession it has will only be temporary. Therefore no steps are reasonably needed to inform individuals of records held about them by the Hub Manager.
- An individual will be able to ascertain information related to records of personal information kept by agencies connected to the DVS Hub in line with these agencies' current practices.
- Commonwealth agencies participating in the DVS are already subject the IPP requirements and the DVS will not change their IPP 5 obligations.

IPP 6 – Access to records containing personal information

- The information retained by the DVS Hub Manager will not include any of the personal information from the message, just reference information about the transaction. Therefore there no provision of access will be required.
- The DVS has no effect on existing avenues for access and correction. Commonwealth agencies using the DVS are already subject to IPP obligations.

IPP 7 – Alteration of records containing personal information

- The DVS Hub does not retain records of personal information therefore no scope for alteration is required. The DVS itself is a means for ensuring the accuracy, currency and completeness of records of personal information provided for enrolment and registration.

IPP 8 – Record-keeper to check accuracy etc of personal information

- The DVS design is essentially about fulfilling this requirement. It is a means to check the accuracy of personal information from a POI document against the database of the issuing agency.
- To the extent that there remains a risk of errors in the information in the document or document issuing agency's database, this is not a risk introduced by the DVS.

IPP 9 – Personal information to be used only for relevant purposes

- The sole use of personal information in the DVS is to verify if details from a document provided as POI correspond to the data records of the document issuing agency.
- This is clearly relevant to the establishment and confirmation of POI.

IPP 10 – Limits on the use of personal information

- Use of personal information through the DVS will be based on consent from the individual concerned.

IPP 11 - Limits on disclosure of personal information

- To the extent that verification through the DVS results in any disclosure of personal information it will be based on the consent of the individual concerned.
- Agencies using the DVS will be required to comply with limits on disclosure under IPP 11 as a condition of use.

8 Privacy Management

It is appropriate to consider options to respond to the possible privacy impacts from the DVS as discussed in the Privacy Impact Assessment section above.

Although the design features of the DVS limit the scope for negative privacy implications from the DVS, the development of management controls and policies for the DVS offer a means to reinforce these.

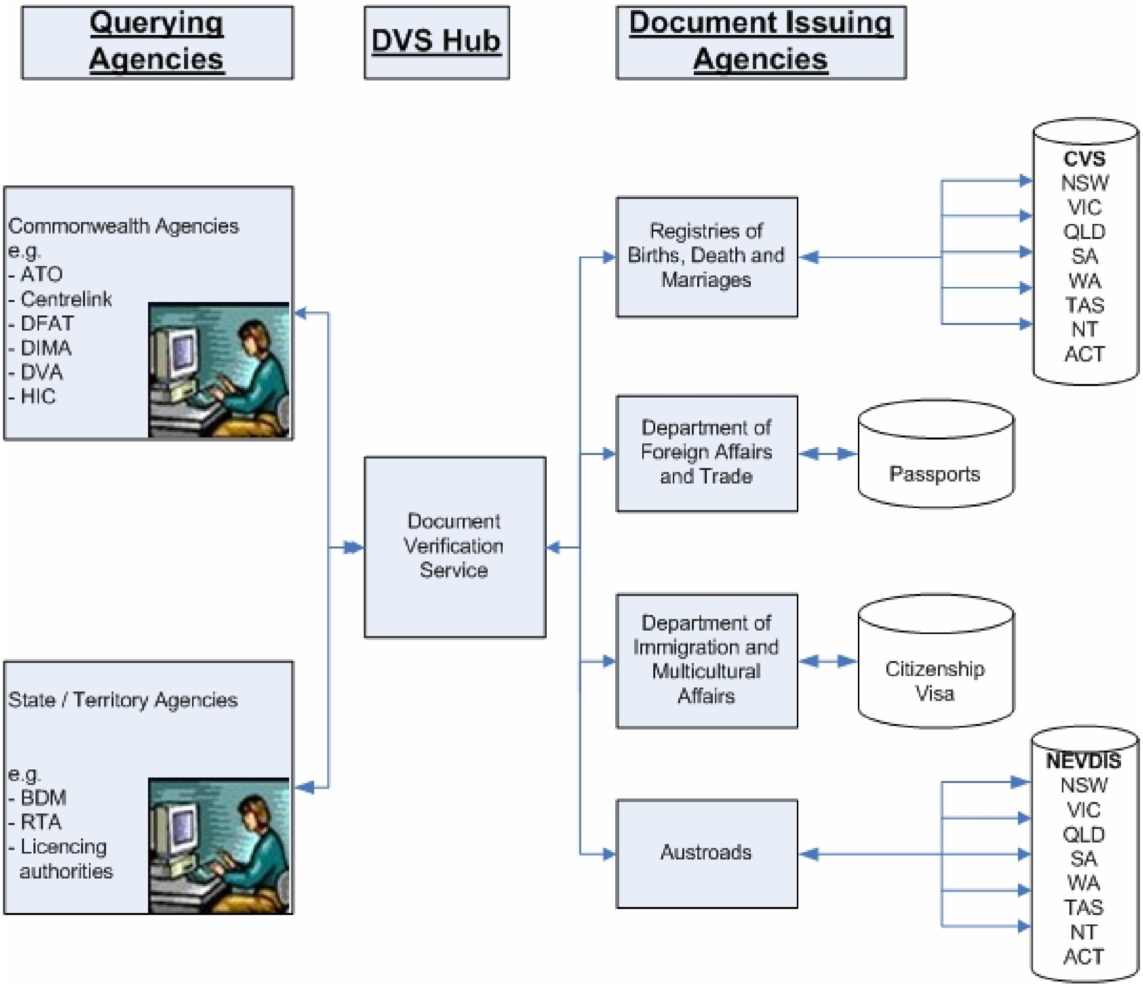
Specific actions to be undertaken in this regard should include:

- Development of standards and protocols to govern DVS administration, access and use including management structure and controls;
- Development of a review and grievance mechanism with assistance from the OPC;
- Development of an audit policy;
- Development of a risk assessment and management strategy for the DVS to include consideration of privacy risks and ongoing responses;
- MOUs with agencies using the DVS to include a requirement to comply with the *Privacy Act 1988* (Cth) including obtaining consent to undertake DVS checks; and
- MOU with Centrelink as Hub Manager to include minimum standards for retention and deletion of personal information, reporting requirements and access controls and require compliance with IPPs.

Such controls and policies are not only useful for management of privacy – they will support the project design and governance framework needed to underpin the development and implementation of the DVS.

ATTACHMENT A

Document Information Service Information Flows


Querying Agencies
DVS Hub
Document Issuing Agencies
Commonwealth Agencies
e.g.
- ATO
- Centrelink
- DFAT
- DIMA
- DVA
- HIC
State / Territory Agencies
e.g.
- BDM
- RTA
- Licencing authorities
Document Verification Service
Registries of Births, Death and Marriages
Department of Foreign Affairs and Trade
Department of Immigration and Multicultural Affairs
Austroads
CVS
NSW
VIC
QLD
SA
WA
TAS
NT
ACT
Passports
Citizenship Visa
NEVDIS
NSW
VIC
QLD
SA
WA
TAS
NT
ACT

.

ATTACHMENT B

Table of Verification Request Details

Document to be verified	Issuing Agency	Document details included in a verification request
Australian Citizenship Certificate and Certificate of Evidence of Australian Citizenship	DIMA	Stock Number Family Name Given names Date of Birth
Birth certificate	Registries of Births, Deaths & Marriages (accessed through CVS operated by NSW Registry)	Year of registration Registration number Family Name Given Names Date of Birth State/Territory
Drivers' licence	Roads and Traffic Authorities (accessed through NEVDIS database operated by Austroads)	Licence number Family name Given names Date of birth State/territory
Australian Passport	DFAT	Passport number Family Name Given names Date of Birth Gender