REPORT
PRIVACY IMPACT ASSESSMENT

IDENTITY VERIFICATION SERVICE
INITIAL IMPLEMENTATION

For: Department of Internal Affairs

17 JULY 2009

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY AND LIST OF RECOMMENDATIONS

1.1 BACKGROUND

The Department of Internal Affairs (DIA) asked Information Integrity Solutions to prepare a Privacy Impact Assessment on the igovt Identity Verification Service (IVS) Programme (Initial Implementation).

The IVS provides a way for people to verify their identity to government agencies online and in real time up to a high level of confidence using an igovt ID. The programme to develop and implement the IVS is part of the All-of Government Authentication Programme which from 1 July 2009 is led by DIA (previously led by the State Services Commission (SSC)).

As part of this initiative SSC developed the concepts of the GLS (soon to be renamed "igovt logon service") and the IVS (soon to be renamed "igovt identity verification service"). The IVS and GLS will work together to provide All-of-Government online authentication solution for individuals. Together, these services fit within a wider system, the current name of which is "igovt". The GLS is operational and the IVS is currently in the Initial Implementation phase.

The current initial implementation of the Limited igovt IVS requirement is to build and deploy the igovt IVS for use by a pilot agency and the public, and to progress the policy/legislation work necessary to support the full service at a later stage. The Initial Implementation of the igovt IVS will only use Evidence of Identity (EOI) source records from New Zealand Passports and Citizenship to issue the igovt ID to users.

1.2 PURPOSE OF PIA

The purpose of the PIA is to identify any potential privacy impacts arising from the Initial Implementation phase of the IVS. The main deliverable is a comprehensive PIA Report for the IVS that includes the evaluation of the privacy risks and the associated implications of those risks along with mitigation strategies. The PIA:

- Independently assesses the proposed service/solution and identified privacy issues against the Privacy Act;
- Identifies the potential effects/risks the igovt IVS may have on personal privacy;
- Independently assesses proposed mitigation options identified in the Privacy Risk Register and by IIS to address such privacy impacts so that the policy objectives of the programme are met and advise which mitigation options should be implemented;
- Identifies any further privacy risks and recommends options for mitigating them;
- Describes any residual or outstanding risks that cannot be addressed through these mitigation mechanisms.

1.3 METHODOLOGY

In preparing this draft PIA report IIS took the following steps:

- Gathered information through phone meetings with DIA, emailed questions and answers and read documents provided (see section 3.4);
- Analysed the information;
- Wrote a draft report;
- Consulted on the draft report with DIA;
- Met other key stakeholders including SSC and the Privacy Commissioner;
- Revised the report based on this additional input.

IIS finalised the report after final comments from DIA. The final stage in the process was for Malcolm Crompton, Managing Director of IIS to present the findings and recommendations of the report to DIA and other stakeholders.

In developing it recommendations IIS has drawn on its "layered defence" approach. This applies a number of possible "tools" to arrive at practical solutions that fit the particular circumstances. The layers and examples of possible tools include:

- "Business as usual" good practice, including education, process and culture change regarding the expectations about the way things are done by staff, and the actions that users need to take to protect themselves;
- Additional law where risks are particularly high, for example, specific use and disclosure limitations, criminal penalties and special measures to ensure review before critical changes are made;
- Technology, including design limits on information collected, what can be connected and who can see what;
- Governance, including transparency and accountability; and
- Safety mechanisms, including easily accessible and responsive complaints mechanisms for Service Users when failure or mistakes occur.

1.4 OVERALL CONCLUSIONS

There key risks associated with a new IT system such as the IVS are that it will:

- Collect or generate more information about individuals than it needs to achieve its purpose (including directly from individuals, indirectly from third parties or via incidental information collected from logs);
- Leave information vulnerable to unauthorised access, use or disclosure;

- Facilitate the ability to connect information about individuals across government (for example, using a unique identifier);
- Create fears about pervasive government surveillance;
- Create rich data sets that increase incentives for using information for new purposes (function creep);
- Leave individuals bearing the burden when things go wrong with the system.

All of these matters contribute to the major fear that individuals have in engaging with these systems: that they will lose control over their information, or that the organisation they have given it to will lose control.

On the information it has so far, IIS considers that DIA has sought to mitigate these risks for the Initial Implementation (and beyond) by building in a number of features consistent with a "layered defence" approach including:

Technology

- Keeping the unique number associated with igovt ID internal to the IVS;
- Using a persistent pseudonym (alias) (Federated Identity Tag or FIT) to deliver identity assertions containing the required attributes to a Service Agency;
- Providing for FITs (FITsa) that are unique to each Service Agency, each service or group of services within a Service Agency, or group of Service Agencies (depending on the particular privacy requirements), called a "privacy domain" or "realm";
- Logically separating the identity authentication function of the GLS from the identity verification function of the IVS;
- Facilitating transparency to Service Users through online access to information (including audit and transaction information) that IVS holds about them.

Policy and process

- Adhering to a number of principles including that:
    - An application for an igovt ID is voluntary;
    - Supply of personal information is only with consent;
    - Maintaining other channels for verifying identity;
    - Physically separating the location of the GLS from that of the IVS;
- Seeking to minimise the information collected, used and disclosed about a Service User to that which is necessary to achieve IVS goals;
- Adopting a policy of maximum transparency to Service Users, including to logging and audit information.

Governance

- Initially intending to keep the governance of the GLS (in SSC) separate from that of the IVS (in DIA.) (However they are both now within DIA).

Law

- In the longer term underpinning the IVS with legislation (the Bill) that limits the purposes for which the igovt ID and associated information can be accessed and used and creates offences relating to the unauthorised access to and use of igovt ID and associated information.

IIS has identified some ways in which the Initial Implementation of IVS could be improved and made some recommendations about these.

IIS considers that the approach DIA has taken, including the transparency measures and the approach to federated identity are among world's best practice for a government provided online identity verification service. However some of the measure outlined above may erode over time, or may not be adequate in the longer term to address the identified privacy risks. As the IVS develops and becomes increasingly relied upon by government agencies for interacting with individuals IIS considers DIA will need to focus on a number of key issues including:

- The governance of the GLS and the IVS now that they are both within DIA;
- The implications of the blurring of the distinction between the GLS and the IVS arising from a number of new GLS/igovt services that the IVS will use; and
- The growing richness of data about individuals' interactions with Service Agencies and the increased incentive to use this information for purposes other than identity management.

IIS has made some recommendations about these issues.

1.5 LIST OF RECOMMENDATIONS

Recommendation 1 – Free text fields

DIA should develop strict business rules about what information can and cannot be inserted into free text fields and what use can be made of this information. DIA should train operators about these rules. DIA should monitor this issue during the pilot and in the long term appoint an auditor to review this information from time to time to ensure that the rules are adhered to and to make recommendations about what action DIA should take if the audit establishes that free text fields contain irrelevant information or that inappropriate use is made of the information.

Recommendation 2 – Audit and logging

DIA should identify the specific purposes for which information generated by IVS activity would need to be logged and audited. DIA should then assess whether each of the activities it proposes to log and audit are required for an identified purpose and then ensure that only those activities that are necessary for those purposes are logged and audited. This process should be a standard process for both the Initial Implementation of IVS and for any further changes proposed in the future. The main focus of decision making should be on what is necessary for promoting or protecting the interests of the Service User.

All such changes should be published prominently and this be done consistent with Recommendation 4 below.

The use and discarding of the passport/citizenship image should be audited to enable DIA to detect any inappropriate use of images and to establish that the process for discarding images is working effectively. (See IVS Privacy Register item PI-026)

Recommendation 3 – Contact information web service (notice and consent)
DIA should ensure that a Service User is informed, at the point where the Service User enters their contact details for GLS purposes, that their contact details may be accessed by other Service Agencies with whom they have an online relationship. DIA should also ensure that applicants for an igovt ID are told that the IVS may access their GLS contact details for specified purposes and their consent obtained.

Recommendation 4 – Informing Service Users
DIA should engage experts in plain language and online useability to ensure that Service Users are easily able to access and understand the important information about how IVS will collect use and disclose information about Service Users. The information Service Users need to know most should be prioritised and made most accessible.

DIA should develop a strategy for publicising changes to the privacy policies and corresponding changes to privacy notices as they occur over time.

Recommendation 5 – Access controls
DIA in the course of the initial testing of the IVS should examine the access controls in place and determine whether they appropriately limit access both to basic identity information and transaction history and other audit logs, taking into account that:

- Access should be strictly on a need to know basis;
- There should be strict monitoring of access to information held on the IVS to deter and detect inappropriate access;
- DIA processes are effective for ensuring that access is withdrawn when DIA staff or others authorised no longer need it because, for example, their role has changed or they have left DIA.

Recommendation 6 – Adequacy of moderate strength logon
DIA should consider as part of its testing during the Initial Implementation pilot whether a moderate strength credential appears to be adequate for IVS purposes and assess the risk of credential compromise.

Recommendation 7 – Helping Service Users correct inaccuracies
DIA should ensure that for Initial Implementation test (and beyond) there is a process for helping Service Users as much as possible to correct any mistakes regardless of the source of the mistake. DIA should monitor whether Service Users have any concerns or complaints about the accuracy of information held in the IVS or about the process for correcting it, and then ensure that in next implementation any problems with the process are addressed.

Recommendation 8 – Managing adverse actions against an applicant or Service User
DIA should ensure (if it does not have one already) that it has a process for managing adverse actions against an applicant or igovt ID holder.

DIA should monitor during the Initial Implementation pilot the circumstances in which a Service User is denied an igovt to assess whether there is a risk of unfair denial based on inaccurate data and to assess the adequacy of processes to address these circumstances if they do arise.

Recommendation 9 – Destruction of captured photo for incomplete applicant
DIA should consider whether there is a good reason for a captured photo (or other information) to be kept when an application for some reason is not completed and if no good reason is identified ensure that processes are in place to delete it.

Recommendation 10 – Contact information web service (use and disclosure)
DIA should ensure that it has the following measures in place in relation to its use of the GLS contact information web service.

- The Service User must be told that the IVS will use the GLS contact information service for specified purposes (in opening a GLS account and when applying for an igovt ID) and asked to give their consent (as per Recommendation 3);
- There must be strict rules (for example, in MOUs and SLAs) about what the IVS can do with the contact information including that it cannot store the contact information in any form;
- IVS must maintains its approach of not storing the contact information in any form, including by ensuring that the IVS does not log any data trails containing email addresses or phone numbers;
- DIA must complete its work of having operating principles in place and oversight mechanisms to ensure that the IVS and the GLS comply with these requirements.

DIA should review the privacy impacts of IVS use of the GLS/igovt contact information service in the PIA DIA conducts on the next stage of IVS implementation.

Recommendation 11 – igovt help desk application
DIA should review the privacy impacts of IVS use of the GLS/igovt help desk application in the PIA DIA conducts on the next stage of IVS implementation.

Recommendation 12 – igovt logon lookup web service
DIA should review the privacy impacts of IVS use of the GLS/igovt logon lookup web service in the PIA that DIA conducts on the next stage of IVS implementation.

Recommendation 13 – Fair allocation of risk

DIA should review the question of Crown liability before the Bill is finalised to ensure that the burden born by Service Users when the IVS fails or problems arise is not unfair. DIA should also ensure that the Terms and Conditions for the IVS fairly allocate risk. Questions that could be asked to help determine fairness include:

- Is the Crown or DIA excluding itself from liability in areas it has main responsibility for and over which the Service User has little or no control?
- Do the provisions mean that the Service User could be substantially out of pocket, or their life substantially disrupted through no fault of their own?
- Will Service Users be required to exercise a level of care that is unrealistic or beyond the average person's knowledge or competence?
- Do the provisions accurately reflect the allocation of responsibility that DIA would be likely to have if a Service User took legal action, or complained to the Privacy Commissioner?
- Are the terms and conditions buried in fine type and framed in language that a Service User is unlikely to find, read or understand?

Recommendation 14 – Governance of GLS and IVS

DIA should put in train steps to consider what might be appropriate governance mechanism to ensure that the necessary separation between the GLS and the IVS is maintained.

2 INTRODUCTION AND OVERVIEW

2.1 BACKGROUND TO PIA

The Department of Internal Affairs (DIA) asked Information Integrity Solutions to prepare a Privacy Impact Assessment on the igovt Identity Verification Service (IVS) Programme (Initial Implementation).

The IVS provides a way for people to verify their identity to government agencies online and in real time up to a high level of confidence using an igovt ID. The programme to develop and implement the IVS is part of the All-of Government Authentication Programme which from 1 July 2009 is led by DIA (previously led by the State Services Commission (SSC)).

The programme encompasses;

- Policy work;
- Standards,
- Government Logon Service (GLS),
- IVS; and
- Future Services.

As part of this initiative SSC developed the concepts of the GLS (soon to be renamed "igovt logon service") and the IVS (soon to be renamed "igovt identity verification service"). The IVS and GLS will work together to provide All-of-Government online authentication solution for individuals. Together, these services fit within a wider system, the current name of which is "igovt". The GLS is operational and the IVS is currently in the Initial Implementation phase.

The current initial implementation of the Limited igovt IVS requirement is to build and deploy the igovt IVS for use by a pilot agency and the public, and to progress the policy/legislation work necessary to support the full service at a later stage. The Initial Implementation of the igovt IVS will only use Evidence of Identity (EOI) source records from New Zealand Passports and Citizenship to issue the igovt ID to users.

A subsequent phase of work will complete implementation of the Limited Service, enhance system functionality, and add the use of EOI source records related to permanent residence (provided by the Department of Labour) to issue the igovt ID to users. This phase is expected to begin in January 2010.

At some time in the future, the full igovt IVS will be implemented. The method for obtaining an igovt ID for the full service will be determined at a later stage. The full service will include enabling legislation.

2.2 PRINCIPLES UNDERPINNING ONLINE AUTHENTICATION

The All-of Government Authentication Program, including the IVS, is underpinned by Cabinet approved policy and implementation principles for government to person (G2P) online authentication.[1] The Policy Principles are:

- Security - Suitable protection must be provided for information owned by both people and the Crown;
- Acceptability - Ensuring that the proposed authentication approach is generally acceptable to potential users, taking into account the different needs of people and emerging industry standards, and avoids creating barriers;
- Protection of privacy - Ensuring that the proposed authentication approach protects privacy appropriately;
- All-of-government approach - Balancing public and agencies' concerns about the independence with the benefits of standardisation while delivering a cost-effective solution;
- Fit for purpose - Avoiding over-engineering, recognising that the levels of authentication required for many G2P transactions will be relatively low;
- Opt-in - Ensuring that members of the public retain the option of authenticating their identity and carrying out transactions offline and are not disadvantaged by doing so. However, it will not be possible for an individual to conduct secure online G2P transactions without the use of the appropriate authentication process.

Implementation principles include:

- User focus - Ensuring the recommended solutions are as convenient, easy to use and non-intrusive as possible;
- Enduring solution - Providing a solution that is enduring yet sufficiently flexible to accommodate change and a wide range of current and future transactions;
- Affordability and reliability - Ensuring the recommended solutions are affordable and reliable for the public and government agencies;
- Technology neutrality - Ensuring a range of technology options is considered, and as far as possible avoiding "vendor capture";
- Risk-based approach - Providing an approach based on agreed trust levels that protects identity and personal information;
- Legal compliance - The solution must comply with relevant law, including privacy and human rights law;

[1] http://www.e.govt.nz/services/authentication/policywork/authprin

- Legal certainty - Relationships between the parties should be governed in a way that provides legal certainty;
- Non-repudiation - The issue of non-repudiation must be considered for those transactions that require it, so that the risk of transacting parties later denying having participated in a transaction is minimised;
- Functional equivalence - Authentication requirements should be similar to those that apply to existing transactions except where the online nature of the transaction significantly changes the level of risk.

These principles demonstrate a strong government commitment to a user-centric and privacy focussed approach. This is reflected in the way that DIA has gone about designing the IVS.

2.3 PUBLIC CONSULTATION

Public consultations commissioned by SSC and conducted in 2007[2] indicate general support for igovt and the proposed identity verification service. In general, those consulted could see the convenience of being able to use it for a wide range of government services. However, the consultation results also underlined the importance of the approach identified in the Cabinet Principles and the need for strong security and privacy measures to ensure community trust and willingness to use the service. Many respondents expressed (among other things) the need for the identity verification service to be user friendly and to have strong privacy and security measures as conditions of their support. Concerns about the extent to which government could be trusted and the possibility of whole of government surveillance were expressed as common themes throughout the consultation.

2.4 STAKEHOLDERS AND ROLES AND RESPONSIBILITIES

The stakeholders involved in the IVS Initial Implementation are:

- State Services Commission (SSC) – The SSC is the Government's lead advisor on New Zealand's public management system and works with government agencies to support the delivery of quality services to New Zealanders. Until 1 July 2009 the Government Technology Services (GTS) section of SSC had responsibility for the government's e-government program and led the All-of Government Authentication Programme. This included responsibility for the GLS. However, since 1 July 2009 the GTS and these responsibilities have been transferred to DIA which has responsibility for the IVS.
- Department of Internal Affairs (DIA) – The DIA is a large government department that has a range of functions. It is responsible for implementing the IVS. It issues passports; administers civil unions; registers births, deaths and marriages; administers citizenship applications; ensures gambling is fair, legal and honest; enforces censorship law and anti-spam law and promotes internet safety; contributes to community development by administering Lottery Grants, Community Grants Schemes, Grants Online and Trusts; and provides support services and policy advice for Ministers of the Crown. It houses the Office

[2] Public consultation about the igovt service *What People Said* March 2008 Prepared for the Department of Internal Affairs by Gatt Consulting.

of Ethnic Affairs, Ministry of Civil Defence and Emergency Management, and the Local Government Commission.

- Births Deaths and Marriages – Births, Deaths and Marriages registers and maintains New Zealand birth, death, marriage, civil union and name change information and provides access to that information by issuing certificates and printouts. The Births, Deaths and Marriages office also appoints marriage and civil union celebrants, and issues certificates of no impediment for people who wish to marry or enter into a civil union overseas. Birth Deaths and Marriages is a section of Identity Services (IDS) of DIA and its online service will be used to pilot the IVS in its Initial Implementation.

- Passports Office – the Passports Office issues and administers passports. It is part of Identity Services (IDS) of DIA and information from its databases will be used to verify the identity of applicants for an igovt ID.

- Citizenship Office – The New Zealand Citizenship Office administers grants of citizenship, confirmation and denials of citizenship, and descent registrations. It is part of the Identity Services of DIA and information from its databases will be used to verify the identity of applicants for an igovt ID.

- Citizens/Service Users – For the IVS Initial Implementation pilot, applicants for an igovt ID will be genealogists and others seeking access to Births, Deaths, and Marriages information.

- Privacy Commissioner – The Privacy Commissioner has been consulted regularly on privacy issues as the IVS has been designed and built.

2.5 GLOSSARY

Term	Description
iDAL	Identity Data Aggregation Layer. These are copies of information from passports and citizenship databases.
IVC	Identity Verified Credential. An alias of an igovt ID. The electronic identity credential provided to users by the IVS.
IVS	Identity Verification Service: The igovt service that provides assertions of user identities based on identity sources controlled by the New Zealand Government Department of Internal Affairs and (in the future) the Department of Labour.
GLS	Government Logon Service: (soon to be renamed “igovt Logon Service”) An all of government shared service to manage the logon process for online

	services of participating agencies. A Service User is transferred to the GLS by the IVS for logon.
FITsa	Federated Identity Tag (service agency) The unique value that identifies the Service User to one Service Agency. While a FIT contains no identity information itself, it is directly related to an igovt ID. For a given Service User, the FIT will be different for each Service Agency. It is synonym for the SAML2.0 NameID. Returned in a SAML2.0 assertion from the IVS as an opaque identifier of the identity of a user in a federated environment.
FLTivs	Federated Logon Tag (for the IVS) A synonym for the SAML2.0 NameID. Returned in a SAML2.0 assertion from the GLS to the IVS as an opaque identifier of the authentication of a user in a federated environment.
EOI	Evidence of Identity: The types of evidence that when combined provide confidence that an individual is who they say they are. (see Evidence of Identity Standard Version 1.0 – June 2006 – soon to be revised)
IDS Contact Centre	This provides support to Service Users for IVS related queries/requests. Staff will try to resolve the problem during the Service User's first call. These calls may come from the igovt helpdesk or directly from the user through the DIA/BDM website. Hand offs can be made to IVS operators if resolution is not possible. This role will include the existing role of SA Help Desk Officer, which provides the capability to secondary authenticate a caller before accessing their IVS record.
Igovt Helpdesk	This Centre provides support for logon (GLS) queries/requests and provides basic information for IVS related calls. Outside of the IDS Contact Centre hours it may provide more support (excluding access to the IVS record) and then the out of hours IVS problems will be forwarded (offline) to the IDS Contact Centre to resolve and call the Service User back.
Logon	(noun) The combination of a username (logon identifier component) with one or more authentication keys (the authentication component) that is authenticated by the GLS when presented by the Service User. (verb) The action a user performs to supply their authentication credentials. The IVS will require a Service User to logon to the GLS.

Privacy Domain	A privacy domain is a SAML2.0 NameID (FLT) generation space. Service Providers that reside in the same privacy domain will be returned the same SAML2.0 (FLT) in the assertion (use) of the Service User's logon in the SAML2.0 response.
SAML	Security Assertion Markup Language - is a XML-based standard that defines messages for communicating a range of security related statements about individual parties, including their authentication.
Service Agency	For the purposes of the IVS a Service Agency is an entity that relies on an Identity Assertion. The entity may be a sector, an individual agency, a set of services within an individual agency or a single service within an individual agency.
VISI	Verified Identity Source Interface: The DIA's EOI source system interface.
SSL	Secure Socket Layer: A protocol for transmitting sensitive information across the Internet in a secure way. The later TLS standard may also be used instead of SSL.
TLS	Transport Layer Security. TLS and its predecessor, (SSL), are cryptographic protocols that provide secure communications on the Internet. There are slight differences between SSL and TLS, but the protocol remains substantially the same. TLS is based on SSL 3.0.
OLEV	Online Life Event Validation. This is a database from which the VISI sources information about the basis on which a passport was granted.
Igovt ID	The igovt ID is an electronic credential that the user can present to government agencies to prove their identity in an online environment.
Service Agency	An Agency providing an online service that uses the IVS to verify the identity of Service Users.

3 THE PIA

3.1 PURPOSE OF PIA

The purpose of the PIA is to identify any potential privacy impacts arising from the Initial Implementation phase of the IVS. The main deliverable is a comprehensive PIA Report for the IVS that includes the evaluation of the privacy risks and the associated implications of those risks along with mitigation strategies. A part of this work will be to meet the objective of assessing whether or not the proposed service/solution for the IVS is consistent with the Privacy Act. The PIA:

- Independently assesses the proposed service/solution and identifies privacy issues against the Privacy Act;

- Identifies the potential effects/risks the igovt IVS may have on personal privacy;
- Independently assesses proposed mitigation options identified in the Privacy Risk Register and by IIS to address such privacy impacts so that the policy objectives of the programme are met and advises which mitigation options should be implemented;
- Identifies any further privacy risks and recommends options for mitigating them;
- Describes any residual or outstanding risks that cannot be addressed through these mitigation mechanisms.

3.2 ASSUMPTIONS APPLIED TO THE PIA

IIS applied the following assumptions to the PIA.

- That its main focus should be on the Initial Implementation of the IVS;
- That is it not necessary or efficient to focus in detail on every possible privacy risk, rather, it is better to focus on the most critical issues, particularly those that have not been resolved;
- That the reader is familiar with the IVS, the GLS and the All-of-Government Authentication Programme;
- That a detailed examination of the Electronic Identity Verification Bill (the Bill) was not required for this PIA;
- That the Bill will not be in force for the Initial Implementation;
- That there will be further PIAs conducted on the IVS;
- That IIS may not have the complete documentation for the IVS and that its analysis could become superseded as more information becomes available;
- That IIS has most of the information that is most critical to its analysis.

3.3 METHODOLOGY

In preparing this draft PIA report IIS took the following steps.

- Gathered information through phone meetings with DIA, emailed questions and answers and read documents provided (see section 3.4);
- Analysed the information;
- Wrote a draft report;
- Consulted on the draft report with DIA;
- Met other key stakeholders including SSC and the Privacy Commissioner;
- Revised the report based on this additional input.

IIS finalised the report after final comments from DIA. The final stage in the process was for Malcolm Crompton, Managing Director of IIS to present the findings and recommendations of the report to DIA and other stakeholders.

In developing it recommendations IIS has drawn on its "layered defence" approach. This applies a number of possible "tools" to arrive at practical solutions that fit the particular circumstances. The layers and examples of possible tools include:

- "Business as usual" good practice, including education, process and culture change regarding the expectations about the way things are done by staff, and the actions that users need to take to protect themselves;
- Additional law where risks are particularly high, for example, specific use and disclosure limitations, criminal penalties and special measures to ensure review before critical changes are made;
- Technology, including design limits on information collected, what can be connected and who can see what;
- Governance, including transparency and accountability; and
- Safety mechanisms, including easily accessible and responsive complaints mechanisms for Service Users when failure or mistakes occur.

3.4 REFERENCE DOCUMENTS AND MEETINGS

In preparing this report IIS has referred to the following documents:

- IVS Privacy Risk Register – completed to March 2009;
- DIA IVS Solution Architecture v0 5;
- IVS High Level Design v0 5;
- Recommended Approach to Ensuring IVC Uniqueness 1.1 27/01/09;
- OPC Response to earlier version of IVC Uniqueness paper – 19/12/08
- Minutes of DIA meeting with OPC approach to IVC Uniqueness 15/01/09
- IVS Business Rules 1.1;
- Get IVC Use Case v1.2;
- IVS Build and Implementation –Appendix 5.4 Initial Implementation Use Case Survey 0.15
- IVS Build and Implementation - Appendix 5.2 Initial Implementation Use IVC Business Use Cases;
- IVS Build and Implementation - Appendix 5.3 Initial Implementation Maintain IVC/GLS Logon Business Use Cases;

- Get Use Case Realisations (UCRs): Apply, Photo Capture, Create, Exceptions;
- Assert UCR;
- Search UCR Specifically for mobile office;
- Cancel igovt ID UCR 1.0;
- View igovt ID UCR 1.1;
- View igovt ID details UCR 1.0;
- UCR0.1 – Operator and Service Agency Provisioning;
- Manage igovt ID 1.0;
- View Audit History UCR 1.0;
- IVS SAML 2.0 Messaging Specification;
- Evidence of Identity Standard Version 1.0 – June 2006;
- Draft terms and conditions for IVS
- Electronic Identity Verification Bill;
- Department of Internal Affairs: Information Code of Conduct;
- IDS Integrity policy
- Draft legal advice on the Identity Verification Service from Crown Counsel 19 July 2006;
- The Privacy Act 1993.

IIS has also taken into account the PIAs that have been done on the All of Government Authentication Service including on the GLS and the IVS. These are:

- Pacific Privacy Partners in 2003. http://www.e.govt.nz/services/authentication/library/docs/authent-pia-200312
- John Edwards in 2005 on the proposed Government Logon Service http://www.e.govt.nz/services/authentication/library/docs/gls-pia/index.html
- John Edwards in 2006 on the proposed Identity Verification Service and is available at http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Identity-Verification-Service-Identity-Verification-Service-Privacy-Impact-Assessment?OpenDocument.

4 DESCRIPTION OF THE IVS PROJECT AND INFORMATION FLOWS

4.1 SUMMARY OF PROJECT INCLUDING BUSINESS NEEDS

The igovt identity verification service will be an all-of-government shared service. It will be a way for online and offline users of government agency services to verify their identity in an online environment in real time. It confirms four verified key attributes; name, date of birth, place of birth and sex. These four verified key attributes make up the igovt ID. The igovt ID is an electronic credential that the user can present to government agencies to prove their identity in an online environment.

The IVS establishes identity as part of the igovt suite of services. The other key part of the igovt services is the GLS. The GLS is an all of government shared service to manage the logon process for online services of participating agencies. The GLS can assure the Service Agency that a Service User using the validated handle 'X' or Federated Logon Tag (FLT) is the same Service User who used the validated handle 'X' or FLT previously. However it makes no "absolute" assertions of identity; that is, it cannot provide uniqueness of a Service User (e.g. that X and Y are not the same individual), nor can it verify external attributes such as name, date of birth, gender or place of birth.

The IVS provides functions that the GLS cannot provide. The IVS adds the concept of absolute identity to the services available to a Service Agency. The IVS seeks to verify that the identity being asserted to a Service Agency is unique. In addition, if asked to do so, the IVS can provide the external attributes of name, date of birth, gender and place of birth.

The IVS is a Service Agency in relation to the GLS. The IVS transfers a Service User to the GLS for logon.

A key design feature of the IVS has been to keep the information the IVS collects to verify identity separate from the information the GLS holds to provide logon services. The GLS has been the responsibility of SSC and DIA is to house and operate the IVS although as indicated earlier, both soon will be housed within DIA.

The stated objectives of the IVS are to:

- provide a single authoritative trusted electronic service for an individual to assert their identity online to participating organisations;
- Protect individuals' privacy by enabling them to control who receives their identity information.

The DIA is testing the concept of the IVS through an Initial Implementation of a limited form of the IVS. The project is to build and deploy the IVS for use by Birth Deaths and Marriages. The pilot is going to target genealogists for the public component of the test but could include others who want to access Birth Deaths and Marriages services online and are willing to attend a mobile kiosk to be issued with an igovt ID. Once the test is complete DIA envisages that the IVS will be scaled up to take on more Service Provider Agencies, to use more sources of EOI (for example Immigration sources in relation to residency) and to expand the eligibility of Service Users to apply for an igovt ID. The Initial limited Service phase is expected to take about 12 months.

DIA will progress the policy/legislation work necessary to support the full service at a later stage.

The initial implementation of the igovt IVS will use Evidence of Identity (EOI) source records from New Zealand Passports and Citizenship to issue the igovt ID to users. To be able to gain an igovt ID, the individual will need to have a valid passport issued, or been granted citizenship, within the last five years.

The set of attributes to be provided by the IVS to the Service Agency will be determined through an agreement between the relevant agencies, and are presented to the Service User for consent before the Service User releases the data to the Service Agency. The Service User cannot selectively restrict access to data. They may only release all the data required by the agency, or choose not to interact with the Service Agency using the IVS.

The IVS will use the current databases of passport and citizenship certificate information for EOI purposes. These are cross-referenced in OLEV and the VISI so that the IVS can ensure that one individual does not create two identities, one based on each document (passport and citizenship certificate).

4.2 IGOVT ID PROCESSES

4.2.1 APPLY FOR IGOVT ID

For the Initial Implementation pilot DIA will travel to particular destinations with mobile equipment to issue applicants with an igovt ID.

Identity is created and an igovt ID will be issued in the Initial Implementation at a DIA mobile office. The applicant will use a self-service computer in the office to apply. The following steps are involved:

- The applicant is asked on the screen to consent to the identity and eligibility checks required during the application process;
- The applicant submits either passport details (last name and passport number) or citizenship details (last name and citizenship certificate number) claiming that the identity presented relates to them;
- The IVS sends the details to the VISI which returns the relevant identity details (first, middle and last names, date of birth, gender and document photograph and the IVS uses these to populate the igovt ID application which is labelled “in progress”. The VISI also checks its Federated ID service to see whether the applicant has been issued with a federated identifier/s (this would be the case if the person has applied before for an igovt ID) and tells the IVS if so;
- The IVS checks the EOI/Uniqueness database to see if there is already an application in train or the applicant already has an igovt ID;
- The IVS again sends the passport or citizenship number to the VISI and the VISI returns details that are relevant to eligibility of the documents for use as EOI. These are: passport/citizenship number, date document issued, date of expiry and document status

- IVS performs an eligibility check (eg was the document issued within the last 5 years? Is it current? Has it been cancelled?);
- The applicant views their name and identity details returned from the VISI and approves them as correct;
- The IVS redirects the applicant to the GLS so they can undertake a moderate strength logon;
- The GLS sends to the IVS a FLT specific to the applicant and to the IVS and indicates the strength of authentication;
- The IVS checks that the FLT is unique across all the existing igovt IDs and igovt ID applications "in progress" and stores the FLT with the created igovt ID application.

4.2.2 PHOTO CAPTURE

After the applicant has completed the Apply process, the next step is for DIA to capture an image of the applicant to be stored with the application. DIA uses this image to confirm the identity of the applicant by matching it with the image retrieved from the VISI which is associated with the passport or citizenship document the applicant has relied on for EOI. The steps in this process are:

- A DIA Officer captures an image of the applicant using software that ensures the image is ICAO compliant;
- The image is digitally signed to verify its source;
- It is uploaded to IVS and the photo capture operator compares the captured photograph with the passport or citizenship photograph provided via the VISI and makes a decision about whether the two photographs match;
- The image capture stage is then complete.

4.2.3 CREATE IGOVT ID

In this stage a second operator compares the photographs, makes a determination and if each of the two operators has determined that the images match, and there are no outstanding investigations in relation to previous steps that have not gone smoothly, the IVS creates an igovt ID for the applicant. If there is one positive and one negative determination, the application is referred for a third determination. Once the application is approved and the applicant has an igovt ID, the passport or citizenship image the IVS has received from the VISI is deleted from the IVS system. The IVS sends the applicant an email, using contact details obtained from the GLS contact information web service, telling them of the application approval. The application process is then complete.

If an application has received two negative determinations on an image, the application is held or declined, the applicant is notified and the application is referred for investigation.

4.2.4 USE IGOVT ID

Once an individual has been issued with an igovt ID he or she can confirm his or her identity online to a Service Agency. This is similar to a person presenting a passport or other proof of identity document in person to a Service Agency. The steps in the process are:

- A Service User goes to an Service Agency web page and wants to use a service;
- The Service Agency asks the Service User to prove their identity and redirects the Service User to the IVS;
- The IVS checks that it knows the Service Agency and then redirects the Service User to the GLS to conduct a moderate strength logon;
- The GLS sends to the IVS the Service User's FLTivs and indicates the strength of the logon;
- The IVS uses the Service User's FLTivs to check if the Service User's igovt ID exists and retrieves the igovt ID that contains the attributes the Service Agency has asked for;
- The IVS shows the Service User the attributes to be sent to the Agency and asks the Service User to agree to them being sent to the Service Agency;
- The IVS checks if the Service User already has a FITsa for the relevant Service Agency/privacy domain and, if not, generates one and prepares a SAML response to the Service Agency;
- The IVS follows the IVS SAML messaging specification to redirect the Service User to the Service Agency with the FITsa and the attributes the Service User has agreed to send.

4.2.5 MANAGE IGOVT ID

The Service User can visit the igovt website and opt to manage their igovt ID. They will be asked to logon using their moderate strength logon (MSL) and then be able to:

- View their igovt ID attributes held by the IVS;
- View their transaction history/igovt ID activity (including identity activity and assertion activity; and
- Cancel their igovt ID online.

Before cancelling an igovt ID the Service User will be warned about the implications.

Once cancelled, the igovt ID cannot be used, but the igovt ID remains on the IVS system. A Service User must again complete the Get igovt ID application process to re-instate their igovt ID. Should the Service User reapply they will receive the same igovt ID (IVCn).

4.2.6 MAINTAIN IGOVT ID AND GLS LOGON

A Service User can also IDS Contact Centre by phone and ask it to can cancel their igovt ID. Before the IDS Contact Centre can cancel an igovt ID or perform any other action at the request of the Service User, the centre must successfully confirm the Service User's identity using their Secondary Authentication. It will mainly do this through a combination of asking the Service User for

something they "know" ie their security questions and answers, and something they "have" such as a call back on a pre registered number or emailing a one time password to a pre registered email address.

If the IDS contact centre operator needs to take an action in relation to a Service User's logon or view their IVS page, the operator can use a GLS/igovt help desk application to access the Service User's igovt web page. The operator asks the Service User their login details and then enters these to enable access. Once the operator has access, he or she will be able to see limited GLS information in relation to the Service User such as:

- Email address;
- Contact details;
- The Service User's GLS transaction history in relation to IVS;
- Filtered logon activity (the operator does not see a Service User's activities associated with online services that IVS does not administer or provide, or activities conducted by a different service agency's version of the igovt helpdesk application).

The IDS contact centre may also use another GLS/igovt logon look up web service to enable a centre operator to connect a Service User to their IVS record.

An IVS Back Office Operator can make some changes to an igovt ID without Service User involvement including:

- To revoke an igovt ID if, following investigation, suspected fraudulent use of an igovt ID is confirmed;
- To record a death manually and deactivate the igovt ID. It will not be reissued at any time unless DIA determines it was incorrect or done in error.

4.3 DETAILS OF INFORMATION TO BE USED BY THE PROJECT

All the information to be collected and used is held, or soon will be held, within DIA within at least four different systems:

- **The IVS** – which enables a Service User to verify their identity online;
- **The VISI** – which provides web services to IVS. It provides an interface between the IVS and various Passport and Citizenship Databases. The VISI is being built to enable the IVS to access passports and citizenship information to establish an igovt applicant's identity. Its services include:
    - **A "person service"** which provides the IVS with the identity details from the passport or citizenship iDALs (including the image (photograph)). It also searches the OLEV to determine whether an applicant presenting a passport also has a citizenship certificate and vice versa. It interacts with the Federated ID Service to determine if a federated identity already exists for the applicant in relation to any of these documents. It passes to the IVS any federated identifiers it finds in the

Federated ID Service. This is a measure aimed at preventing a person from having two igovt IDs based on two different sources of EOI. It enables the IVS to determine if the identity presented is unique;

- **A Federated ID Service** which maps and stores an individual's passport identity number and/ or citizenship identity number with a federated identifier (VISI number) – one for each kind of document the OLEV has indicated that an applicant has. This is a privacy measure aimed at ensuring that passport and citizenship identifiers are contained within the passports and citizenship environment and not stored in the IVS. The Federated ID service gives the federated identifier/s to the IVS to store with the igovt ID in a Uniqueness Database.
- **A travel document service** that provides the IVS with the passport details that enable the IVS to determine eligibility (it does not store this information). These details are obtained from the Passport iDAL which is a copy of the original passport application database;
- **A Citizenship certificate Service** that provides the IVS with the citizenship details that enable the IVS to determine eligibility (it does not store this information). These details are obtained from the Citizenship iDAL which is a copy of the original citizenship application database;

- **The Passport System and the Citizenship System** - which hold information about individuals issued with Passports and Citizenship documents;

- **The GLS** – which enables an igovt ID holder to authenticate themselves to a Service Agency using an opaque identifier called a Federated Logon Tag (FLT) which the IVS has mapped against the igovt ID. The GLS also provides a web service that enables the IVS to get a Service User's contact information eg email address for various administrative purposes. The GLS also has a web service to allow logon lookup and an igovt helpdesk application to allow the IDS Contact Centre to provide logon support to an IVS Service User.

The other entity or entities that are involved in the IVS process is the Service Agency asking the Service User to validate their identity.

The following are diagrams that demonstrate in broad terms the information held in each system/entity and the information flows.

Each of these systems or entities collects/holds/uses the following information.

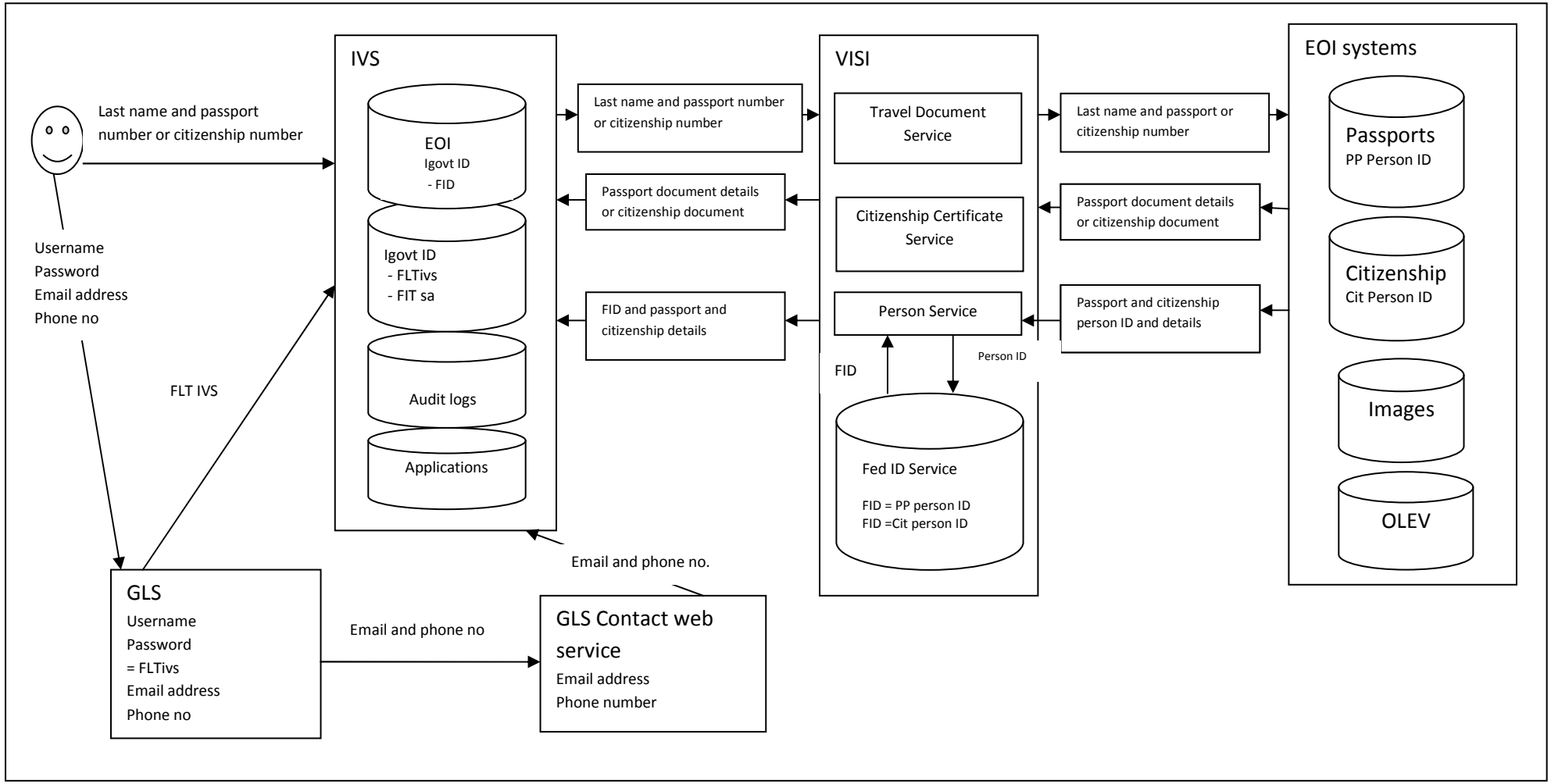
DIA				Service provider (Agency)
IVS	**VISI**	**Passport and Citizens Source Systems**	**GLS**	

Application
• Full Name
• Date of birth
• Gender
• Place of birth
• Passport or citizenship document number (from which type of EOI used can be inferred)
• Date and time of application
• Status of IVC application
• Reasons relating to status
• Passport/Citizenship Photo (until application completed then discarded)
• other notes
• Flags (eg review by back office needed)
• Igovt ID status
 	
Captured Photo
 	
Igovt id
	Federated ID system
	• Fed ID No
	• Passport and or Citizenship ID No
	• Federation type
	• Consumer ID ie IVS
	• ID No for Passports service and or
	• ID No for citizenship service
	
	Person Service
	• No information stored audit logs only kept.
	• transit through:
	  • EOI transaction reference
	  • Fed ID
	  • Federation already exists
	
	Travel Document Service
	• No information stored audit logs only kept.
		Passport iDAL
		• Passport person ID
		• Passport document ID
		• Passport application ID
		• Passport photograph
		• Passport document number
		• Passport first name, middle name, last name
		• Passport date of birth
		• Passport place of birth
		• Passport gender
		• Passport date issued
		• Passport date expiry
		• Passport status
		
		Images
		• Passport person ID
		• Passport Document ID
		• Passport Image
		
		OLEV
		• Passport application ID and Passport document ID Cross referenced
			• FLTivs
			• Other FLTs associated with the logon
			• User name (chosen by user and not validated)
			• Email address
			• Mobile phone number (for MSL)
			• Other optional contact information
			• Second factor authentication – security question
			• Token - serial number
			
			Audit logs
				• FITsa
				• Agency identifier
				• Chosen identity attributes could include up to:
				  ○ Name
				  ○ Date of birth
				  ○ Gender
				  ○ Place of birth
				
				Audit logs

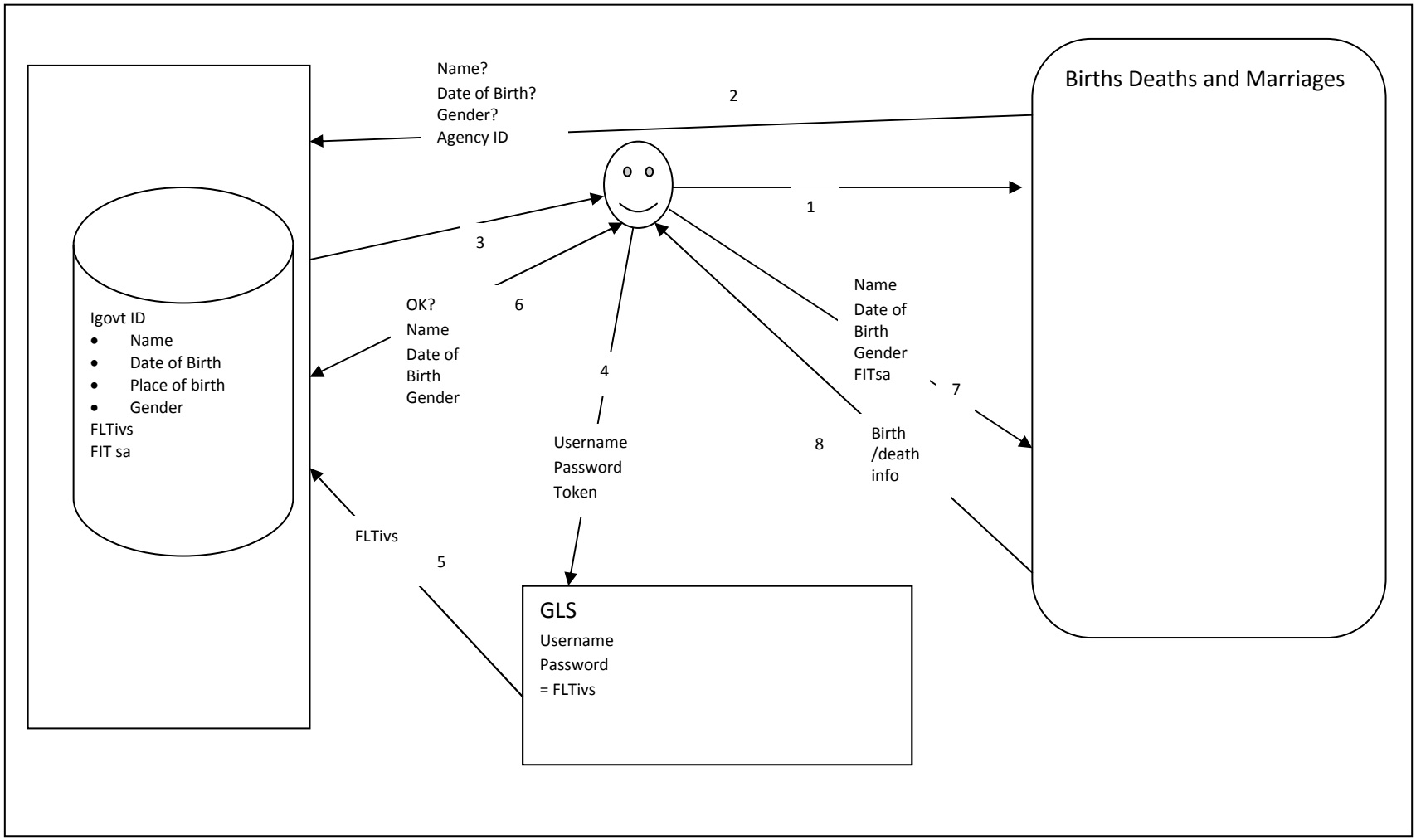
• IVCn (random number not shown to Service User) • Name • Date of birth • Gender • Place of birth • FLTivs • FITsa (includes code to indicate which agency/privacy domain, one for each SA to which the identity has been asserted) **EOI database** • IVCn • Fed ID (passport) • Fed ID (citizenship) **Audit logs** • Transaction history	**Audit logs database** **Citizenship Certificate Service** • No information stored audit logs only kept.	citizenship certificate ID **Citizenship iDAL** • Citizenship Person ID • Citizenship certificate ID • Citizenship first name, middle name, last name • Citizenship date of birth • Citizenship place of birth • Citizenship gender • Citizenship photograph • Citizenship date effective • Citizenship type • Citizenship status **Audit logs**		

4.4 DATA/INFORMATION FLOW DIAGRAMS

4.4.1 GET IGOVT ID



4.4.2 ASSERT IDENTITY



4.5 IDENTIFICATION OF WHO WILL ACCESS THE DATA/INFORMATION

The following entities will have access to the following information

Entity	What can be accessed/viewed

Service User	Igovt ID attributes
	
	Full access to transaction history such as:
	• Assertions;
	• Any Service User activity on IVS page;
	• Renewal of igovt ID;
	• Who else has viewed the Service User's record eg IVS Operator;
	• Any time IVS status is updated either manually or by the system or personal details changed;
	• Some information about investigation activity. Still being worked out but likely to be:
	  o Tell that application has been referred for back office for further processes;
	  o Not tell if sent for investigation; but
	  o Tell once the necessary action has been taken and completed.

Service Agency	Pre-defined reports - Service Agency can run these from a web page in which they can see transactions in relation to their own services. These are usage based eg number of assertions made – no identifying information.
Mobile Office Operators	Will only be able to see information relating to the particular application they are dealing with.
Exceptions Desk Operator (EDO)	Handles exceptions arising during an igovt ID application. Can see all audit information up to the point where the exception arises during an application. Can flag an application and add notes eg reason for referral for investigation.
IDS Contact Centre	Provides support for IVS related queries and requests. Staff will have access to: a) the Service Agency Helpdesk Application: includes information required to perform a secondary authentication of the caller; username, contact details, token ID, logon transactions with IVS (not any other SA's), and security questions; b) IVS system: includes view access to summary screens of both the

	igovt id and related applications. Final role definitions have yet to be defined but could also include access to transaction history in order to answer SU enquiries.

5 POSSIBLE PRIVACY RISKS IDENTIFIED

IIS has identified the following possible risks that could arise in relation to the IVS Initial Implementation. The numbers included refer to the IVS Privacy Register.

Privacy Principle	**Possible risk**
Lawful purpose, collection necessary (1)	The IVS collection is not for lawful purpose connected with a function or activity of the agency.
	That IVS collects more information than it needs for the purpose of verifying the identity of individuals online, for example: • Via data logs and audit trails that particularly over time shed light on the wider interactions of an individual with government as per PI-008.
	That the IVS will result in other organisations collecting more information than they need for the purposes of the services they provide online , for example, use the IVS when a much lower level of authentication would be adequate (as per PI-002).
Direct collection (2)	Risk that information in the IVS about an individual is collected indirectly and without their knowledge or consent for example: • A Service Agency seeks access to a Service User's igovt ID without the Service User's knowledge or consent.
Notice/Transparency (3)	That information about individuals could move through the IVS without individuals being aware of what happens to the information.
Unfair, intrusive collection (4)	This is unlikely to become an issue.
Storage and security (5)	Risk that sensitive information will be available to IVS staff, for example, the igovt contact centre etc which could make it vulnerable to unauthorised access, use or disclosure as per PI-006a or alteration as per PI-006c Risk that if a person's credential is compromised the person's IVC could be vulnerable to fraudulent misuse.

Access (6) Correction (7)	Risk that individuals will not know what information is held about them and hence be unable to take action to correct it if it is wrong. (also as per PI-006)
Accuracy (8)	Risk that people may be unfairly denied the opportunity to gain or retain an IVC due to mistakes or inaccurate information held about them – for example, comparison of passport photo with photo captured by the IVS.
Retention (9)	Risk that information will be held longer than it needs to be.
Limits on use (10)and disclosure (11)	Risk that information collected from one source is used out of context and possibly inaccurately to make decisions about an individual's life in another area, with no chance of review or knowledge by the individual for example: • Use of IVS information about what Services a Service User has contacted for law enforcement purposes; • Inferences unrelated to identity drawn from igovt ID attributes.
	Risk that IVS could use or disclose information collected for one purpose for purposed unrelated to the original purpose of collection, for example: • use of contact information collected for GLS purposes, used for IVS purposes as per PI-004; • Use of passport and citizenship information.
Unique identifiers (12)	Risk that IVC might become the sole means of identifying or authenticating individuals for example through: • Gradual reduction in other ways/channels of authenticating (as per PI-003).
	Risk that the IVS as a unique identifier could facilitate the linking, matching and sharing of information about individuals in ways that were not possible before and which may not be welcome or acceptable to individuals. For example through: • Use of the GLS for authentication; • The VISI and linking of person records with citizenship information with passport information which was not linked before as per IP-012a; • Moving GTS from SSC to DIA which will bring GLS into the DIA

	with the IVS as per PI-023.
Allocation of risk	That when mistakes or problems occur in the IVS process individuals' lives are severely disrupted and the individual must bear the burden of ensuring that errors are rectified.
Function creep	That the functions of the IVS will evolve in ways that come to be regarded as unwelcome and unacceptable function creep.

6 FINDINGS ON PRIVACY RISKS AND PRELIMINARY RECOMMENDATIONS

The following section analyses the IVS against each of the privacy risks identified above. It includes a brief analysis of the IVS against the relevant Information Privacy Principle under the Privacy Act. It makes recommendations to address identified risks.

6.1 PURPOSE OF COLLECTION AND IPP 1

6.1.1 COLLECTION FOR LAWFUL PURPOSE

IIS notes the legal advice that DIA received on 19 July 2006 (the legal advice) and has not identified any reason to explore this issue further.

6.1.2 COLLECTION NECESSARY FOR PURPOSE

IIS considers, in line with the legal advice, that the design of the IVS pilot has generally sought to limit the information "collected" for IVS to that which is necessary for the function of the IVS. The information collected for the application for an igovt ID and made available to Service Agencies is information intimately associated with identity and the means of establishing that it is unique. It discards photo information collected from Passports and Citizenship once a successful match has been made.

IIS has identified some possible risks in the IVS that could result in more information collected than necessary. These arise in relation to:

- The fields associated with the igovt ID where free text can be added;
- The audit trails that the IVS could generate;
- The circumstances in which Service Agencies use the igovt ID.

6.1.2.1 FREE TEXT FIELDS

Where there are areas to insert fee text notes against an application for an igovt ID there is a possible risk that information could be included that contains subjective views or other information that is not relevant to the IVS.

Discussions with DIA indicate that there are good reasons to have free text fields where Officers can make notes. In particular it allows decisions made to be more thoroughly reviewed. Key areas where free text is allowed include:

- Requiring an officer in a mobile office to give a reason for why they have flagged an application for further investigation – which helps to ensure the officer thinks about why they have put that flag;
- Investigators providing notes about the outcome of their investigation including about the recommendation for action that has been made – which assists review of the outcome and action taken;
- Operators making notes if they don't follow a recommendation made by investigator – which also assists with review of the decision made;
- Notes to be made if a person wants the igovt contact centre to cancel their igovt ID – which assists with review.

IIS considers that there is justification for having free text fields. It is important that DIA is accountable for key decisions made in relation to an individual's igovt ID. However, IIS considers that it is an area that requires close scrutiny to ensure that the notes remain strictly relevant and as objective as possible. IIS understands that apart from incomplete applications, DIA does not delete anything from the IVS.

Recommendation 1 – Free text fields
DIA should develop strict business rules about what information can and cannot be inserted into free text fields and what use can be made of this information. DIA should train operators about these rules. DIA should monitor this issue during the pilot and in the long term appoint an auditor to review this information from time to time to ensure that the rules are adhered to and to make recommendations about what action DIA should take if the audit establishes that free text fields contain irrelevant information or that inappropriate use is made of the information.

6.1.2.2 AUDIT

It appears that all, or nearly all, activities in relation to the IVS will be logged and audited. IIS understands that there had not been a structured decision making process for deciding what activities should be logged and audited and what should not. IIS notes that DIA is now in the process of addressing this matter.

A key risk with the IVS is that through the logs it generates it might be possible to build up a picture, particularly over time, about how a Service User has interacted with government This issue has already been identified by the Office of the Privacy Commissioner and in the IVS privacy register item PI-008.

IIS considers that there are strong security and accountability reasons why extensive auditing would be necessary. These include:

- To enable a Service User can keep track of their interactions;
- To enable a Service user to see who else has accessed their igovt ID record;

- To enable DIA to monitor compliance with role based access rules;
- To enable Service Agencies to have information about access to their services via the IVS;
- To detect unauthorised access, use, or disclosure either by internal or external people;
- Certain evidentiary and forensic purposes.

However, unless there is a structured process for assessing what will or will not be logged and audited there is a risk that some information will be collected that is not necessary for these or other important purposes of the IVS.

Recommendation 2 – Audit and logging
DIA should identify the specific purposes for which information generated by IVS activity would need to be logged and audited. DIA should then assess whether each of the activities it proposes to log and audit are required for an identified purpose and then ensure that only those activities that are necessary for those purposes are logged and audited. This process should be a standard process for both the Initial Implementation of IVS and for any further changes proposed in the future. The main focus of decision making should be on what is necessary for promoting or protecting the interests of the Service User.

All such changes should be published prominently and this be done consistent with Recommendation 4 in section 6.3 below.

The use and discarding of the passport/citizenship image should be audited to enable DIA to detect any inappropriate use of images and to establish that the process for discarding images is working effectively. (See IVS Privacy Register item PI-026)

6.1.2.3 Unnecessary collection of attribute information by Service Agencies

There is a risk, as identified in IVS Privacy Register PI-002 that the IVS will result in a Service Agency collecting more information than it needs for the purposes of the services it provides online. For example, the Service Agency might use the IVS when a much lower level of authentication would be adequate, or ask for more attributes than it needs for the particular service.

DIA has addressed the risk of unnecessary collection of the igovt ID and attributes to a significant extent by minimising the attributes associated with an igovt ID, by enabling a Service Agency to pick and choose which attributes it requires for a particular service, and also by including in the design the concept of a "privacy domain" which enables a Service Agency to enter into separate arrangements with the IVS for the different services it provides. This enables a Service Agency to interact separately with the IVS for each of those services in terms of the federated identifiers used and the attributes it receives. DIA also proposes a number of measures for the implementation phase to address the issue. These include:

- Conducting a security assessment of Service Agencies proposing to use the IVS to determine the security level and the suitability of the IVS for the particular service; and
- The development of MOUs and agreements with Service Agencies.

IIS considers that addressing this issue will be critical to maintaining community trust in, and the integrity of, the IVS system. It is strongly linked to the other key issue with the IVS (to be discussed below at section 6.11) of the wider risk that the igovt ID could become a widely used unique identifier.

In terms of a layered defence to address this risk, the DIA has built in a range of technical design and process features that are likely to be sufficient for the purposes of addressing these risks associated with the Initial Implementation phase. However, this is such an important issue that there should be measures in place to ensure into the future that Service Agencies only use the IVS and relevant attributes associated with an igovt ID when they really need to.

IIS considers that significant other layers of defence are required to address this risk in the longer term including:

- Mechanisms to prevent a service agency from participating in IVS and receiving particular attributes unless the service it is providing justifies it;
- "End to end" or "whole of information cycle" monitoring and accountability mechanisms to ensure that all participating agencies, including Service Agencies, use the igovt ID the way they agreed they would use it;
- Complaints mechanisms for Service Users who believe they are being required to use an igovt ID when it is not justified.

IIS considers that the Bill, which is to be in effect by the time the IVS is more fully implemented, will be an important measure to help address this issue. For example, it:

- Has a purpose clause (clause 3) which says that the legislation is intended to ensure that participating agencies can achieve a high degree of confidence in an individual's identity through the use of an igovt ID <u>if a degree of confidence is necessary for the interaction</u> (referring to the provision of the service);
- Has principles, for example, clause 4 that says that information will only be provided to the participating agency with the consent of the person concerned, and even if that consent has been obtained, the IVS can supply only the minimal personal information about the individual to the agency and only information that is necessary for the agency to act as part of a given transaction;
- Requires DIA and Service Agencies to take these principles into account in making decisions under the Act (clause 1(2);
- Establishes a regime whereby agencies become "participating agencies" for the purposes of the legislation if those agencies are listed in regulations made under the Act. A decision to include the agency in the regulations would need to take into account of the purpose clause and principles;
- Gives the Chief Executive the power (clause 43) to set standards or specifications for use of electronic credentials by participating agencies and the power to suspend use of the igovt ID

by an participating agency if satisfied that these standards or specifications have not been complied with (clause 45);

- Provides that a person may complain to the Privacy Commissioner if the person believes that the Service Agency has obtained information other than in accordance with the Bill (clause 50).

Assessment of the Bill is outside the scope of this PIA so IIS does not make any recommendation about this. These provisions appear to make a good start in addressing this issue. However, in the long term IIS considers that DIA should ensure that it has in place the layered defence mechanisms outlined above. There is a risk that unless there are specific processes outlined either in law or regulation for assessing whether an agency is appropriately seeking to use the IVS such processes may fade away or be diluted over time.

IIS considers that the Chief Executive should set standards and specifications for use of the IVS under clause 43 of the Electronic Identity Verification Bill. This should include a requiring the agency to demonstrate that use of the IVS and relevant attributes is justified taking into account the identity risk associated (using the EOI Standard) with use of the particular online agency service.

IIS also considers that the Chief Executive should use s 44 of the Electronic Identity Verification Bill to require Service Agencies to monitor their use of the igovt ID and report annually on the findings of such monitoring.

6.2 DIRECT COLLECTION AND IPP 2

In the Initial Implementation, the IVS will access information about a Service User indirectly from a number of sources. These include:

- EOI information from Passports and Citizenship;
- Service User contact details from the GLS contact information web service.

In future implementations the IVS will access death information from the Births Deaths and Marriage database to avoid fraud and to keep the IVS database current.

Indirect collection can create privacy risks particularly if an individual does not know about the collection and would be unlikely to agree to it. It can result in an individual losing control over information about them. If individuals do not know who holds information about them, they cannot correct it if it is wrong or seek redress if wrong decisions affecting their lives are made on the basis of that information.

In the case of the EOI information the IVS collects from Passports and Citizenship, IIS considers (in line with the legal advice) that the requirements of IPP 2 are met, and the privacy risks mitigated, by the fact that the IVS proposes to make the fact that its collection of information from Passports and/or Citizenship very transparent and permission based by:

- Telling the applicant that it will collect information from Passports and/or Citizenship, and getting express consent; and

- Displaying the information received from Passports and/or Citizenship in an application window, and asking the Service User to confirm its accuracy.

The risk is further mitigated by the fact that there are other channels by which individuals can verify their identity. IIS considers that the risks of indirect collection are sufficiently mitigated by these measures. However, it is worth noting that the impact of alternative channels recedes as government increasingly relies on the igovt ID as its favoured way of doing business with Service Users and other channels become less convenient and accessible.

In the case of IVS access to contact information from the GLS contact details web service, the risk of indirect collection can be mitigated by transparency and consent. However, there may be other risks associated with the GLS contact information web service, for example, that it may undermine the separation between the IVS and the GLS. This is discussed in section 6.11.

Recommendation 3 – Contact information web service (notice and consent)
DIA should ensure that a Service User is informed, at the point where the Service User enters their contact details for GLS purposes, that their contact details may be accessed by other Service Agencies with whom they have an online relationship. DIA should also ensure that applicants for an igovt ID are told that the IVS may access their GLS contact details for specified purposes and their consent obtained.

6.3 Notice and transparency and IPP 3

DIA appears to have every intention of being as transparent as possible about the matters outlined in IPP3, including in cases where information is collected indirectly. The real privacy risk arises out of the manner in which transparency is achieved. It is all too common for key matters to be buried in fine print in terms and conditions, or in unintelligible language in lengthy privacy notices many clicks away from where Service Users access a service.

The key strategies for ensuring Service Users receive the information they need include:

- Using clear and non legalistic language;
- Designing web pages so that the particularly important information is placed where it is most meaningful and likely to be read by the Service User (for example, at the point where information is entered);
- Adopting a layered notice approach consistent with the approach adopted by Privacy Commissioners globally (www.privacyconference2003.org/resolution.asp and www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf).

IIS notes that IDS has already implemented a layered notice approach in giving privacy information about its services.

Recommendation 4 – Informing Service Users
DIA should engage experts in plain language and online useability to ensure that Service Users are easily able to access and understand the important information about how IVS will collect use and disclose information about Service Users. The information Service Users need to know most should be prioritised and made most accessible.

DIA should develop a strategy for publicising changes to the privacy policies and corresponding changes to privacy notices as they occur over time.

6.4 UNFAIR AND INTRUSIVE COLLECTION AND IPP 4

IIS has no information to indicate that this is likely to be a risk arising in relation to the IVS.

6.5 STORAGE AND SECURITY AND IPP 5

6.5.1 ROLE BASED ACCESS

A key security risk with a new IT system holding sensitive personal information is that it will be inappropriately accessed by those who do not need to see it. It could result in identity fraud or connecting of information that should not be connected (this is discussed further below in section 6.11.1).

Documentation that IIS has seen so far indicates that provision for role based access has been built into the technical design of the IVS. IIS has set out its understanding of the current approach to who can access what information on the IVS and in what circumstances in section 4.5. DIA is still developing this policy. IIS understands that DIA has established procedures for provisioning and de-provisioning DIA or other authorised users of their systems. The key will be to ensure that the access roles and the particular information available to each is appropriate.

To the extent that such access has been determined, DIA appears to have limited access appropriately to ensure that DIA officers are only able to access the information that they need to access.

Recommendation 5 – Access controls

DIA in the course of the initial testing of the IVS should examine the access controls in place and determine whether they appropriately limit access both to basic identity information and transaction history and other audit logs, taking into account that:

- Access should be strictly on a need to know basis;
- There should be strict monitoring of access to information held on the IVS to deter and detect inappropriate access;
- DIA processes are effective for ensuring that access is withdrawn when DIA staff or others authorised no longer need it because, for example, their role has changed or they have left DIA.

6.5.2 SECURITY OF A SERVICE USER'S CREDENTIAL

IIS considers that the security of a Service User's GLS credential is a potentially vulnerable point in the IVS. A compromised GLS credential could make a Service User's igovt ID vulnerable to use by someone other than the Service User.

IIS assumes that this issue has been considered as part of security risk assessments conducted for the IVS and a moderate strength credential has been considered adequate for IVS purposes. This may need to be reviewed as igovt IDs become more widely used with consequentially greater impact on a Service User of such a compromise increases and greater value to thieves.

Recommendation 6 – Adequacy of moderate strength logon

DIA should consider as part of its testing during the Initial Implementation pilot whether a moderate strength credential appears to be adequate for IVS purposes and assess the risk of credential compromise.

6.5.3 SEPARATE VISI PERSIST STORE

The IVS Privacy Register identifies a possible privacy issue arising from having a VISI persistent identifier store that is separate from the IVS and Passports and Citizenship. On the information available to it, IIS cannot see any obvious privacy risks around this as long as the store is properly secured with strict access controls and governance measures. The VISI is currently covered by the protections in legislation covering passports and citizenship processes and there will be agreements between passports and citizenship and the IVS on access to and use of the information exchanged between them. IIS considers that these measures are likely to be adequate, but suggests that this could be a matter examined in later PIAs once the pilot is completed and DIA is moving to the next phase of IVS implementation.

6.6 ACCESS BY SERVICE USER TO INFORMATION HELD IN THE IVS AND IPP 5

A key tool to give individuals control over personal information held about them by others is to enable the individual to gain access to that information. The Bill (clause 17 and clause 21) makes clear provisions for a Service User to gain access to:

- Core identity information held in the their igovt ID and associated information; and
- His or her igovt ID usage history (including who other than the Service User has accessed the history).

There are limited circumstances in which a Service User might not be able to access information about every authorised person who has accessed their record, for example, where that access would prejudice an investigation or prosecution against that individual for an offence involving the use of the electronic identity credential.

IIS has outlined in section 4.5 what information a Service User will have access to. This is

- Igovt ID attributes (as they stand if the Service User were to assert at the time of viewing)
- All transaction history such as:
  - Assertions;
  - Any Service User activity on IVS page;
  - Renewal of igovt ID;
  - Who else has viewed the Service User's record eg IVS Operator
  - Any time IVS status is updated either manually or by the system or personal details changed
  - Some information about investigation activity. Still being worked out but likely to be:
    - Tell that application has been referred for back office for further processes;
    - Not tell if sent for investigation but
    - Tell once the necessary action has been taken and completed.

In the initial implementation, Service Users will not have access to the photograph attached to their igovt ID. However, in line with the Bill as currently drafted, the IVS will provide such access in later implementations.

A Service User will logon at moderate strength to the GLS and then they will be able to see this information via their igovt account page. The information will be presented in two tabs. One will display general identity activity and interactions with the IVS including:

- Date and time of activity;
- The Service Agency connected with the transaction;
- The action involved (eg request to view igovt activity, FITsa generated for Service User, igovt ID created, etc);
- Who carried out the action (eg Service User, IVS system, IVS operator, IDS Contact Centre, user name of operator).

The other tab will display information about each assertion of identity a Service User has made. It will show:

- Date and time of assertion;
- Service to which the assertion was made;
- The attributes provided in the assertion and those not requested.

IIS considers that apart from the igovt ID photograph, Service Users will gain access to all relevant information relating to their IVS related transactions and that the IVS is to be congratulated on its transparent and best practice approach.

6.7 CORRECTION AND IPP 7

A key reason for an individual to gain access to a record is to enable them to see if the information held is correct and up to date and to be able to correct the information if it is wrong or add information if information is out of date. IIS notes that the Bill specifically provides for a Service User to be able to access their IVS record to see if it is correct and up to date (clause 4(e) principle, clause 17(b), clause 26(1)(d)).

For the Initial Implementation, if a Service User finds that attribute information is wrong the Service User will be referred back to Passports or Citizenship to have the information corrected there. This is because the IVS obtains this information from the VISI which has passed on information obtained from Passports or Citizenship databases. The IVS Privacy Register PI-006c identifies as a privacy risk the fact that for the Initial Implementation the Service User will be required to go to the information source, that is, Passports and Citizenship to correct any information.

The risk IIS identifies here is that the Service User might be passed between Citizenship or Passports and the IVS with no one taking responsibility for the mistake or for fixing it. It is not clear yet how likely it is that Service Users will need to take steps to correct information held on the IVS about them.

Recommendation 7 – Helping Service Users correct inaccuracies
DIA should ensure that for Initial Implementation test (and beyond) there is a process for helping Service Users as much as possible to correct any mistakes regardless of the source of the mistake.

DIA should monitor whether Service Users have any concerns or complaints about the accuracy of information held in the IVS or about the process for correcting it, and then ensure that in next implementation any problems with the process are addressed.

6.8 ACCURACY OF INFORMATION HELD IN THE IVS AND IPP 8

There is possible risk that an individual might be unfairly denied the opportunity to gain or retain an igovt ID due to mistakes or inaccurate information held about them. As discussed above, it is not clear how likely it is that mistakes could occur or that information held in the IVS about a Service User could be inaccurate. There could be a risk that an applicant is wrongly rejected because of an assessment that the captured photo does not sufficiently match the photo provided from Passport and Citizenship. However, IIS considers this risk is low given that the Get IVC UCR sets out an extensive procedure for assessing photographs, which includes the possibility for photos to be assessed by up to three IVS operators. In future implementations DIA proposes to have behind the scenes facial recognition matching as further back up.

Another possibility is that a Passport or citizenship document has been issued to someone who has adopted the applicant's identity with the exception of the photograph used. This is also probably a low risk. However, the Bill (clause 32) has another strand of defence to address this risk by providing for a process that the Chief Executive must follow before suspending or revoking an igovt ID. This includes notifying the Service User of the possible suspension or revocation and the reasons for it, and giving the Service User the chance to make written or electronic submissions.

IIS understands that DIA will have for the Initial Implementation test a process for managing adverse actions against an applicant and this will include providing reasons for rejecting an application or revoking an igovt ID and a chance for the Service User to respond to this. It will also include DIA reports to the Office of the Privacy Commissioner.

It is unclear at this stage how likely it is that a Service User would be unfairly denied an igovt ID because of inaccurate information.

Recommendation 8 – Managing adverse actions against an applicant or Service User
DIA should ensure (if it does not have one already) that it has a process for managing adverse actions against an applicant or igovt ID holder.

DIA should monitor during the Initial Implementation pilot the circumstances in which a Service User is denied an igovt to assess whether there is a risk of unfair denial based on inaccurate data and to assess the adequacy of processes to address these circumstances if they do arise.

6.9 RETENTION OF IVS INFORMATION AND IPP 9

IIS understands that the IVS will retain nearly all the information held in the IVS permanently. IIS assumes that for fraud prevention reasons in particular, significant amounts of information held in the IVS will need to be kept indefinitely. However, each item of information should be analysed against identified purposes and a decision made about what information should be stored and for how long. IIS has identified one possible issue relating to the retention of a captured photo in circumstances in which an application is not, or cannot be completed. In some cases it might be

necessary to keep such a photo for fraud prevention purposes, however, this will not always be so, for example, if a person simply changes their mind about applying.

Recommendation 9 – Destruction of captured photo for incomplete applicant
DIA should consider whether there is a good reason for a captured photo (or other information) to be kept when an application for some reason is not completed and if no good reason is identified ensure that processes are in place to delete it.

6.10 Limits on use and disclosure IPP 10 and 11

6.10.1 Use or disclosure of IVS information for purposes unrelated to the purposes of IVS

A possible risk in relation to the very useful and high integrity identity information to be held about individuals in the IVS is that it might be accessed /disclosed and used for purposes unrelated to the purposes of the IVS.

IIS notes that the Bill (clause 49) has set specific limits on who can access information in the IVS. For example, it limits access to the photo stored in the IVS to the following:

- The individual him or herself;
- The Chief Executive or an employee authorised by the Chief Executive;
- An officer of a law enforcement agency for the purpose of any proceedings relating to an offence relating to the igovt ID or a computer system on which the operation of the IVS database relies.

The Bill (clause 21) also limits access to the record of igovt ID usage history to specified individuals and circumstances. Unless there is a warrant, those seeking access must (in summary) satisfy the Chief Executive that access is necessary for the purpose specified in the Bill.

- The individual to whom the igovt ID usage history relates;
- A law enforcement agency in circumstances similar to those for law enforcement agencies specified above;
- The conduct of proceedings relating to the igovt ID or the IVS;
- Statistical or research purposes where the only de-identified information is published;
- A person authorised by the Chief Executive who is carrying out administrative, technical or other functions relating to the management, maintenance, and use of the IVS.

IIS considers that it is appropriate for Law Enforcement Agencies to have access to information relating to a particular transaction a Service User has conducted with a Service Agency that is suspected as fraudulent. The Bill appears to allow this. It is consistent with the approach taken in the Privacy Act.

However, there is a question about the breadth of purposes for which law enforcement access should be allowed.

For example, IVS will have information in its logs about what services a Service User has made assertions to and the time and dates of such contact. This could be of interest to law enforcement agencies that have detected fraud in relation to one Service Agency and then seek to find out what other agencies that particular identity has contacted. Law enforcement agencies might seek access to IVS information in cases where an individual has had unsuccessfully applied for, or had difficulty applying for, an igovt ID, for wider law enforcement intelligence purposes. Patterns of other usage history and photographs might also attract interest.

More broadly, there is the risk that law enforcement may wish to seek access for broad sweeps through IVS covering a large proportion of the population or other mass inquiry/analysis arrangements.

A concern is that there appears to be some ambiguity in how these provisions apply to law enforcement access. For example, it is not clear that the Bill would prevent access by law enforcement agencies to information about an unsuccessful applicant as the definition of "usage history" only covers information about the use of an igovt ID once it is obtained. It does not appear to include processes before a person obtains an igovt ID. Also, it is not clear how closely related to IVS operations and purposes a law enforcement investigation must be to allow access.

Allowing to liberal access to law enforcement agencies could undermine community trust in the IVS and generate fears of wide ranging government surveillance. As a result, a very clear policy on law enforcement access and how requests for expansion of access are to be addressed when such proposals arise is vital.

This risk is probably low for the Initial Implementation but could be significant once the full IVS is implemented. Comment on the Bill is outside the scope of this PIA, however, in the long term IIS considers that DIA should ensure that the circumstances in which law enforcement agencies can gain access to IVS information are clear and unambiguous and as far as possible directly related to the functioning, administration and integrity of the IVS system.

IIS notes that the Bill has specific provisions in the Bill limiting the purposes for which a Service Agency can use an igovt ID and associated attributes and information to that of verifying and individual's identity by electronic means (clause 18).

IIS considers that the provisions in the bill significantly address the risk of use or disclosure of usage history information and photographs held on the IVS for unrelated purposes by Service Agencies. A key additional protection is ensuring that Service Users are able to see through their igovt ID web page what access has been had to their record and by whom (to the extent that this does not prejudice an investigation).

6.10.2 Risk of unrelated use by IVS of information collected by others

6.10.2.1 Information collected by Passports and Citizenship

The IVS uses information collected by Passports and Citizenship for purposes unrelated to its original purposes of collection.

DIA has lowered this risk and met its obligations under the Privacy Act by gaining the consent of the Service User. The risk is further reduced by the fact that individuals can choose not to use the IVS

and use other channels to verify their identity. In the context of the Initial Implementation these protections should be adequate to address the privacy risk, but once the IVS is more widely implemented the best protection would be to authorise such use by law and provide specific protections around it including for the operation of the VISI.

6.10.2.2 CONTACT INFORMATION COLLECTED BY THE GLS

Through its use of the GLS/igovt contact information web service, IVS will use contact information collected by the GLS for purposes unrelated to those for which the GLS collected it. Using this service the IVS will be able to access a Service User's email address and preferred contact phone number. It proposes to use this information for notifying an applicant that their application has been successful (or not), and for other administrative purposes, for example, that an igovt ID has been revoked. There is probably not a high risk of harm for Service Users in this, indeed there may be a good deal of convenience and benefit. However the risk is that the Service User is surprised that the IVS is able to contact them and may wonder how the IVS got their contact details. This may lead the Service User to further reflect on what other information about them may be shared between different government services. A further concern is that this sharing of information may undermine the original intention that the GLS and the IVS should maintain strict separation of roles. IIS considers that there must be a number of measures in place to address these risks.

Recommendation 10 – Contact information web service (use and disclosure)

DIA should ensure that it has the following measures in place in relation to its use of the GLS contact information web service.

- the Service User must be told that the IVS will use the GLS contact information service for specified purposes (in opening a GLS account and when applying for an igovt ID) and asked to give their consent (as per Recommendation 3 in section 6.2);
- there must be strict rules (for example, in MOUs and SLAs) about what the IVS can do with the contact information including that it cannot store the contact information in any form;
- IVS must maintains its approach of not storing the contact information in any form, including by ensuring that the IVS does not log any data trails containing email addresses or phone numbers;
- DIA must complete its work of having operating principles in place and oversight mechanisms to ensure that the IVS and the GLS comply with these requirements.

DIA should review the privacy impacts of IVS use of the GLS/igovt contact information service in the PIA DIA conducts on the next stage of IVS implementation.

6.10.2.3 LOGON INFORMATION COLLECTED BY GLS

IDS Contact Centre operators will have access to an igovt help desk application that will enable it to provide logon support services to IVS Service Users. This means that IVS operators will have access to a Service User's GLS logon page and some information collected there for purposes unrelated to IVS service. There are risks that IVS operators could see more information than they need for providing support to IVS Service Users. There are also risks if such access could be obtained without a Service User's knowledge or consent. This is also another possible means by which the separation between the IVS and the GLS could be undermined.

The application has a number of measures in its design to address some of the risks. For example it limits what the IVS contact centre operator can see to:

- the details about the Service User's IVS account; and
- Filtered logon activity – that there is logon activity, but not what agencies the logon relates to.

The application only enables support for everyday functions associated with logging on to the IVS, such as forgotten password, forgotten username, forgotten mobile phone number and problems with how to use the GLS etc. The contact centre will not be able to delete a logon, suspend a logon or change the user name for a logon.

In addition, the GLS/igovt logon service audits all access to a Service User's logon via the GLS/igovt help desk application, and a Service User can view this access in their online activity report.

IIS considers, on the information it has available to it at this stage, that these measures, combined with the fact that such access would only be available to a contact centre operator if the Service User has provided the necessary credentials and so is fully aware of the access, are sufficient to mitigate the privacy risk. The service is clearly one that could be of significant benefit to Service Users in that it enables the contact centre to provide a "one stop shop" type service and may avoid Service Users having to make two separate phone calls to address a particular problem. However, IIS has not looked at this service in detail and believe further review would be helpful at a later stage in the implementation of the IVS.

Recommendation 11 – igovt help desk application
DIA should review the privacy impacts of IVS use of the GLS/igovt help desk application in the PIA DIA conducts on the next stage of IVS implementation.

6.11 Unique identifiers and IPP 12

6.11.1 IVS unique identifier

The IVS creates a unique identifier for each person that successfully applies to be able to validate his or her identity online. There are a number of significant privacy risks associated with unique identifiers and IPP 12 seeks to address some of these risks. IIS notes the legal advice that IPP 12 does not prohibit the assignment of a unique identifier in the context of the IVS. IIS considers that the IVS appears to comply with the requirements set out in IPP 12 in that:

- The igovt ID is exclusive to the IVS and is not one that has been assigned to an individual by any other agency;
- The IVS has extensive processes in place to ensure that an igovt ID is only assigned after the identity of an individual is clearly established; and
- An igovt ID is kept internal to the IVS and not disclosed outside it.

The key risk associated with a unique identifier, particularly in the context of a service aimed at facilitating online identity validation across government (or more widely) is that it could become the means to link information about an individual's interactions with government or other organisations

in ways that was not possible before. It could enable an agency or organisation to compile an extensive profile on an individual's life which could be used for a wide range of purposes unrelated to the purposes for which the individual gave the information. The information to be linked could be that which the individual consciously agreed to give, as well as the incidental information generated by data trails which can reveal rich information about behaviour without the individual's knowledge. DIA has sought to mitigate this risk by building in a number of features consistent with a "layered defence" approach including:

Technology

- Keeping the unique number associated with igovt ID internal to the IVS;
- Using a persistent pseudonym (alias) (Federated Identity Tag or FIT) to deliver identity assertions containing the required attributes to a Service Agency;
- Providing for FITs (FITsa) that are unique to each Service Agency, each service within a Service Agency, or group of Service Agencies (depending on the particular privacy requirements), called a "privacy realm";
- Logically separating the identity authentication function of the GLS from the identity verification function of the IVS.

Policy and process

- Adhering to a number of principles including that:
    - An application for an igovt ID is voluntary;
    - Supply of personal information is only with consent;
    - Maintaining other channels for verifying identity;
    - Physically separating the location of the GLS from that of the IVS.

Governance

- Initially intending to keep the governance of the GLS (in SSC) separate from that of the IVS (in DIA.) (However they are both now within DIA).

Law

- Underpinning the IVS with legislation (the Bill) that limits the purposes for which the igovt ID and associated information can be accessed and used and creates offences relating to the unauthorised access to and use of igovt ID and associated information (clause 52).

These strategies are consistent with a layered defence approach and significantly reduce the risk that the unique number associated with the igovt ID will be used to link information about an individual across a range of government organisations. The use of FITs makes it practically much more difficult for those connections to be made and the legal framework deters such linking by creating offences, provides oversight by the Chief Executive and creates transparency and accountability through reporting requirements.

The Bill will not be in place for the Initial Implementation, but IIS does not consider this is of major concern given the limited scope of this first phase and the presence of the Privacy Act to regulate the handling of personal information relating to the IVS.

The design of the IVS and the policies underpinning it appear, on the information IIS has available to it, to be generally adequate to address the risks associated with the Initial Implementation test. IIS notes that the measure outlined above of keeping the governance and physical location of the GLS separate from that of the IVS could be undermined by the movement of GTS, the section of SSC responsible for the GLS, into DIA. As of 1 July 2009:

- GTS will merge with IDS in DIA, which is responsible for managing the IVS;
- The GLS and the IVS will be physically housed in Datacom facilities but in separate cages with stringent separate access controls;
- The GLS will be managed and supported by Datacom with DIA having no direct access to GLS systems;
- The IVS will be managed and supported by DIA.

IIS considers that for the purposes of the Initial Implementation test, the measures in place, including the governance measures within DIA, will be adequate to address any possible privacy risks resulting from this merger. However, this may not remain the case as the IVS evolves. This is discussed below.

6.11.2 Use of Passports and Citizenship identifiers

Use of Passports and Citizenship unique identifiers by the IVS for the purpose of verifying identity information and establishing uniqueness raised some privacy concerns and is a case in point of the potential for a unique identifier to be used to link information about an individual for purposes unrelated to the original purpose of its creation. However, for the purposes of the Initial Implementation of IVS, IIS considers that there are sufficient measures in place (already discussed above, such as consent, and the use of FITs) to mitigate the privacy risks associated with such use.

IIS considers that the measures in place are likely to be adequate to address the privacy risks posed by the Initial Implementation for the IVS and possibly the early stages of full implementation.

6.11.3 Use of logon lookup web service

IIS understands that the IVS is considering using the GLS/igovt logon lookup web service for its IDS Contact Centre. The centre might use this in cases where it cannot associate a caller needing support with their IVS record. The most accurate means of matching a caller with their IVS record is using their FLTivs, but the caller does not know this. The contact centre would ask the Service User their GLS username and then use the web service to obtain from the GLS the Service User's FLTivs. The user name is a unique identifier that could be used to link information about a Service User across agencies.

This service also has a number of privacy measures built in to it. However, IIS has not had the chance to examine these in detail.

IIS considers that this raises significant privacy risks and would require, at the minimum the kind of measures it outlined for the GLS/igovt contact details service. For the purposes of the Initial Implementation test, IIS makes no recommendation. However the use of the service should be explored further.

Recommendation 12 – igovt logon lookup web service
DIA should review the privacy impacts of IVS use of the GLS/igovt logon lookup web service in the PIA that DIA conducts on the next stage of IVS implementation.

6.12 UNFAIR OR INAPPROPRIATE ALLOCATION OF RISK

It is a common feature of many new IT systems that those implementing it pay significant attention to managing their own risks, but often forget to consider and manage the risks that the system might pose for Service Users. Some of the most common ways this occurs is:

- Terms and conditions that disclaim any liability on the part of the service provider for any failure in the system and for any loss, or damage that might be suffered by the Service User as a result;
- Placing significant responsibilities on the Service User in relation to the information they provide and its protection;
- Uncoordinated customer support mechanisms which means that the Service User is passed between various Service Agencies, none of whom will take responsibility for the problem, or for ensuring, particularly where more than one Service Agency is involved, that addressing the problem is coordinated and then finally resolved;
- Hard to access, unresponsive and often hostile complaints mechanisms.

All of these mean that Service Users will find themselves having to bear all the inconvenience, disruption to life and cost of resolving their problem and restoring order to their lives.

6.12.1 CUSTOMER SUPPORT

There is significant potential for a Service User's life to be disrupted through failure of the IVS, particularly as online interactions with government and other organisations for key services become increasingly the norm. It is critical to ensure that the IVS takes appropriate responsibility for preventing and addressing mistakes and failure and has top class coordinated customer support available 24/7.

However, managing this issue is a complex issue in this case because of the relationship between the IVS and the GLS. Solving problems in a coordinated way may require some ability for the one person to have access to both. IIS notes the GLS web services discussed above that the IVS proposes to use which will enable the IVS to help Service Users with logon problems as well as IVS problems in a "one-stop-shop" service. However, as noted above, particularly in later implementations of the IVS extreme care will need to be taken to ensure that this does not undermine the privacy protections so critical to having a strict separation between the two. IIS understands that DIA has an excellent customer support culture; however it has not had the chance to look at this in detail.

6.12.2 TERMS AND CONDITIONS

IIS has only seen early versions of terms and conditions and is not in a position to comment in detail on these. However, IIS notes that the Bill (s 57) seeks to protect the Crown and its employees from liability in relation to loss or damage due to the use of an igovt ID. It might be valuable to review this provision with the question of whether this unfairly allocates too much risk to the Service User. The

risk if this balance is not got right is that Service Users will be unwilling to use IVS for fear that if something goes wrong they will be left having to bear financial or other loss or damage. This issue was raised by the Office of the Privacy Commissioner. This risk includes Crown liability issues that require careful thought and legal advice.

Recommendation 13 – Fair allocation of risk
DIA should review the question of Crown liability before the Bill is finalised to ensure that the burden born by Service Users when the IVS fails or problems arise is not unfair. DIA should also ensure that the Terms and Conditions for the IVS fairly allocate risk. Questions that could be asked to help determine fairness include:

- Is the Crown or DIA excluding itself from liability in areas it has main responsibility for and over which the Service User has little or no control?
- Do the provisions mean that the Service User could be substantially out of pocket, or their life substantially disrupted through no fault of their own?
- Will Service Users be required to exercise a level of care that is unrealistic or beyond the average person's knowledge or competence?
- Do the provisions accurately reflect the allocation of responsibility that DIA would be likely to have if a Service User took legal action, or complained to the Privacy Commissioner?
- Are the terms and conditions buried in fine type and framed in language that a Service User is unlikely to find, read or understand?

6.13 Function creep

There is always a risk that there will be an expansion of functions in the IVS beyond those stated to be its purpose, again impacting on citizen trust and confidence.

Whether or not expansions will be welcome or accepted by the community or seen as unwelcome "function creep" will depend on their nature and how they are made. The difference may simply be the speed of introduction, the degree to which the community is taken into confidence and other subtle matters. At other times, the difference is more real and will never be considered as anything but function creep because it is seen as an inappropriate invasion of privacy, for example if the changes were introduced with insufficient surrounding governance mechanisms such as transparency and accountability mechanisms to ensure abuse or unintended consequences do not happen.

In relation to IVS IIS considers there is a risk that a number of the measures aimed at ensuring customer control and preventing unrelated secondary uses of IVS could to erode over time. As the IVS becomes more widely used, and agencies increasingly rely on online identity verification, the consent measure will become less effective as a means of privacy protection if the cost and inconvenience of alternatives increases. As the transaction data becomes increasingly rich and informative about individual behaviour when interacting with government there may be increased incentive to overcome the technical and other barriers to accessing and connecting information

across government. There could be strong incentives to extend the use of the IVS to the private sector.

6.13.1 Effectiveness of consent

IIS considers that DIA is to be congratulated for the extent to which Service User consent has been built in to the IVS. But as has been pointed out in previous PIAs the power of choice as a privacy risk mitigation mechanism will inevitably erode overtime particularly if the IVS is successful and widely taken up, and online government services consequently expand. In the ongoing search for greater efficiencies it is likely that other channels for validating identity will slowly fade away. For convenience and these other reasons individuals will be increasingly locked into using the IVS.

The significance of this is that, in the long term, DIA will need to rely on the other privacy "tools" to address privacy risk. In particular there must be strong governance and accountability measures backed up by strong safety net mechanisms for when failure occurs. The Bill is a good start, but the governance mechanisms are likely to need strengthening as identified above.

6.13.2 Increasing richness of data

As the IVS becomes increasingly used, it could create an increasingly valuable source of data. The greater the value, the increase in incentives to hurdle the practical barriers created by the use of FITs and FLTs to prevent connection of information about an individual between agencies.

IIS explored the question of the strength of the current technical barriers and has concluded that there are very significant technical barriers to connecting up an end to end transaction that a Service User conducts with an agency and then to connect a range of end to end transactions between agencies. Doing so would require cooperation between a number of sections of DIA, a deep knowledge of how the various pieces of information could be linked together and significant amount of time. Merging the GLS with the IVS would also be a difficult and expensive exercise. The Bill will also create legal barriers for use of IVS information for purposes other than verifying identity in the online environment.

However, there are several possible gaps in protection that could become more significant in the future. With the movement of GTS section of the SSC into the DIA all the key elements of the online identity management system (including Passports and Citizenship) will be located within DIA. This has significant potential to undermine trust in the system. It will be significantly harder for the community to be convinced that information will not be linked and shared. It also reduces the potency of the Bill as the Chief Executive will have the power to make crucial decisions about both the GLS and the IVS and there is significant potential for there to be a conflict of interest particularly in areas where there is some discretion. Also, unlike for the IVS, there is no specific legislation governing the GLS. There is clearly significant developments being proposed in the kinds of services offered by the GLS and these could gradually further undermine the separation between the IVS and the GLS and in the absence of a legal framework this to occur, this change happen without real public knowledge or examination of the overall impact of what is happening.

This is an issue mainly for future implementations of the IVS. However, IIS initial thinking on this issue is that, separating the GLS from the IVS is a major lynch pin in the protection against inappropriate linking of information about igovt ID users across agencies and other organisations. As such, in the long term, the governance of the GLS and the IVS should be separate from DIA and

possibly separate from each other. Another possibility is to keep the current arrangement but establish a separate section within DIA, or other appropriate agency to maintain independent oversight of the identity management system as a whole (or possibly just the IVS and the GLS) with terms of reference that include ensuring that the original cabinet principles underpinning the system are upheld and identifying points at which further privacy impact assessment are needed.

Recommendation 14 – Governance of GLS and IVS
DIA should put in train steps to consider what might be appropriate governance mechanism to ensure that the necessary separation between the GLS and the IVS is maintained.

7 CONCLUSIONS

IIS considers that on the information it has to hand so far DIA has taken significant steps to address the possible privacy risks associated with the Initial Implementation of the IVS. IIS has not identified any major concerns in relation to the information supplied so far in the Initial Implementation design or process. It has identified some ways in which the Initial Implementation could be improved and has made recommendations about this.

IIS has identified some longer terms risks which will need further consideration in the context of further phases of implementation of the IVS and of the All-of-Government Authentication Programme as a whole.