PRIVACY IMPACT ASSESSMENT

OF

IGOVT IVS FULL SERVICE BUILD

For: The Department of Internal Affairs (NZ)

19 September 2012

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

1.1 BACKGROUND

The Department of Internal Affairs (DIA) asked Information Integrity Solutions (IIS) to conduct a Privacy Impact Assessment (PIA) on the full service build of the igovt Identity Verification Service (igovt IVS). IIS conducted a PIA on the igovt IVS initial implementation phase in December 2009. DIA also asked IIS to conduct an assessment of privacy risks of the extension of the use of igovt services to the private sector through the partnering arrangement with New Zealand Post Limited (NZPost), which is a State Owned Enterprise.

The igovt IVS is a key enabler of the New Zealand government's Result 10, ensuring New Zealanders can complete their transactions with government easily in a digital environment.

The igovt IVS Full Service build project has been initiated to deliver the full igovt IVS service offering. This includes meeting the legislative requirements in the Electronic Identity Verification (EIV) Bill. This Bill was introduced to Parliament in August 2011, passed the first reading on Tuesday 12 February 2012 and has been reported on to Parliament by the Government Administration Committee on June 12 2012. The project also includes meeting DIA obligations under its partnering agreement with NZ Post.

1.2 PURPOSE

DIA asked IIS to conduct a PIA of the proposed enhancements to the igovt IVS including use of immigration and birth data and the use of NZ Post for the photograph and capture stage to ensure the service build is compliant with the Privacy Act.

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

The PIA also provides a privacy assessment of the extension of use of igovt services to the private sector. This will occur, for example, through the use of the igovt logon service by the provider of Common Web Services to NZ government agencies. It will also take place through the RealMe service being developed in partnership with NZ Post that will leverage existing igovt services. RealMe is the official digital verification and authentication service that enables individuals to access, manage and present their identity and personal information when interacting with NZ enterprises and government agencies online.

The PIA provides a general assessment of this kind of extension of use and makes a specific assessment of planned use of the igovt logon service by the Common Web Services platform. However, it does not make a detailed assessment of RealMe at this stage as DIA is proposing to conduct a detailed PIA on this in the near future.

1.3 METHODOLOGY

In conducting the PIA IIS took the following steps:

- consulted with DIA and finalised the work plan;

- gathered and read information about the igovt IVS full service build;
- met with key stakeholders including:
    - DIA staff;
    - NZ Post;
    - the Privacy Commissioner;
- analysed the data;
- prepared draft reports which DIA reviewed;
- had further meetings to clarify some matters;
- prepared the final report.

1.4 POTENTIAL RISKS

The potential risks of an identity information management system such as the igovt 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.

1.5 OVERALL CONCLUSIONS

Overall, IIS considers that the igovt IVS full service build has maintained the design features that seek to address these risks. DIA has maintained its approach of only collecting, using and disclosing personal information about igovt ID applicants and holders that is necessary for the purposes of the igovt IVS and of discarding any information that is no longer necessary to hold.

The main new privacy risks arise from the fact that individuals can use additional Evidence of Identity (EOI) sources on which to base their application for an igovt ID. These sources, which are birth and immigration data, are not as robust as those for current applicants and are not seamlessly integrated with the igovt IVS in the way that passports and citizenship identity source systems are. The mechanism for establishing uniqueness has also become more complex. This has meant that there is a much greater reliance on back office system manual checking and the need to scan key identity documents into the igovt IVS. It has also meant that specific individual agency identifiers such as a

licence number or document number printed on documents are stored permanently in the igovt IVS (as part of the scanned image). Introducing NZ Post into the igovt ID application process has also required some changes that could introduce privacy and security risks.

The privacy risks IIS identified relating to the igovt IVS full service build and made recommendations about include:

- that the storing of scanned documents, which have printed on them non source EOI agency identifiers such as driver licence identifier or building licence number or document numbers, could undermine the principle of keeping agency specific individual identifiers separate from the igovt IVS. It could increase security risks and create additional interest from law enforcement agencies;
- a possible loss of transparency about the way applicants' information is handled due to the increased number of hands through which the information will be passed;
- increased security and privacy risks due to human error or malicious intention arising from the increase in manual handling of applicants' information;
- possible loss of ability for individuals to access information held about them in the igovt IVS, for example, scanned documents;
- possible security risk and loss of applicant control at the point where the applicant attends at a NZ Post office at the photo capture stage;
- the need to ensure reports of igovt IVS operations are restricted to those consistent with the purposes of the igovt IVS;
- the need to ensure that information about igovt ID status (other than revocation) is only given to agencies for purposes consistent with those of the igovt IVS;
- the risk that complaints and inquiry mechanisms are not adequate to meet the more complex arrangements of the igovt IVS full service build.

IIS also identified key issues that could arise in relation to the extension of use of igovt services to the private sector, including NZ Post's RealMe and made a recommendation about this. However IIS notes that DIA will be conducting a detailed PIA on RealMe and so it did not make detailed comments and recommendations on this.

It also considered privacy issues around the use of the igovt logon service by a private sector Common Web Service Provider and made a recommendation about this.

1.6 RECOMMENDATIONS

IIS made the following recommendations.

Recommendation 1 – Independent and coherent governance structure for use of igovt services
IIS recommends that as a matter of priority DIA develops a coherent governance structure for managing the evolution of igovt services and their use by public sector, quasi private sector, and private sector organisations. The governance structure should include a mechanism for community

and private sector stakeholders to participate in decision making about use of igovt services and the terms and conditions of such use. The roles and functions for the governance structure should include:

- a person responsible for oversight of end-to-end and big picture privacy issues as igovt services evolve and become accessible to a wider range of users;
- development of coherent policies and requirements relating to the management and implementation of privacy for all igovt service users;
- oversight of the terms and conditions on which new organisations integrate to ensure that the current high standard of security and privacy requirements are maintained and implemented in a consistent way;
- the establishment and implementation of mechanisms to monitor compliance with the policies and requirements by all users of igovt services;
- the development and implementation of formal and coherent and accountable processes for managing change and dealing with function creep;
- establishing an ongoing mechanism for involving of the community and the private sector in decisions about the evolution of use of igovt services.

Recommendation 2 – Common Web Service Provider use of igovt logon service
IIS recommends that:

- the Common Web Service provider is transparent about the fact that it is using the igovt logon service;
- where a Common Web Service provider using the igovt logon service also provides other identity related services to DIA, DIA ensures that the service provider has strict access controls in place that prevent any system administrator (or other person) from having a view of more than one of these services;government employees using the Common Web Service and igovt logon service have easy access to one-time-password tokens so that they can have more than one moderate strength logon if they choose to do so; and
- as identified strongly in the extension of igovt services to the private sector analysis, there are appropriate governance mechanisms to oversee terms and conditions for use of igovt services and to ensure the privacy impacts of change are assessed.

Recommendation 3 – Technology: Encryption of scanned documents and governance for access
IIS recommends that if scanned documents are to be stored in the igovt IVS they should be stored in encrypted form with very limited access to the encryption keys. There should be strong governance and accountability mechanism for deciding when access to the scanned EOI documents will be allowed. The EIV Bill should be amended to cover access to scanned documents as well as photographs.

Recommendation 4 – Technology: Reduce reliance on scanned documents
IIS recommends that DIA works with DoL and any other New Zealand agencies that are sources of EOI to develop the technology necessary to reduce the need for EOI and related documents to be stored in the igovt IVS. DIA should also determine when these documents will be no longer needed and a process for deleting them from the igovt IVS at that point.

Recommendation 5 – Business as usual and technology: Audit and logging
DIA (in conjunction with NZ Post where appropriate) should ensure there is a process for assessing which activities in the full igovt IVS build should be audited and logged. The process should ensure that activities are only logged if there is good reason consistent with the purposes of the igovt IVS full service build.

Recommendation 6 – Business as usual: Informing Service Users
DIA should engage experts in plain language and online usability to ensure that Service Users are easily able to access and understand the important information about how igovt IVS and NZ Post (and any other participants) 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 privacy policies and corresponding changes to privacy notices as they occur over time.

Recommendation 7 – Business as usual: Expert advice to assess and manage security risks in manual processing
IIS recommends that once the igovt IVS back office processes are more fully spelled out, DIA engage a security expert at both the development and implementation stage to assess the security risks of the processes and advise on how to minimise these risks.

Recommendation 8 – Accountability: Regular monitoring and audit of back office processes
IIS recommends that once policies and procedures for back office processing are in place, DIA regularly monitors, and conducts audits of, them to ensure that staff comply with them.

Recommendation 9 – Technology: Balance between User access and protection through encryption
IIS recommends that scanned documents and photographs stored in the igovt IVS should be stored in an encrypted form.

Recommendation 10 – Business as usual: Policies, procedures and training for staff to avoid inaccuracies in data entered into the igovt IVS
IIS recommends that, to minimise inaccuracies in igovt IVS data, DIA and DoL develop detailed policies, procedures and training for igovt IVS back office staff and DoL staff involved in verifying information supplied by igovt ID applicants and other processes involved in the verification and image determination stages of an igovt ID application process.

Recommendation 11 – Safety-net: Helping Service Users correct inaccuracies
IIS recommends that DIA provides easily accessible help for individuals seeking to correct their igovt ID using the processes provided for in the EIV Bill. DIA should monitor the incidence of inaccuracy of information held in the igovt IVS in order to identify and address any inaccuracy problems with its or DoL's administrative processes relating to the application and issuance of igovt IDs.

Recommendation 12 – Business as usual and technology: Deletion of scanned documents when automated processes available

IIS recommends that DIA develops a schedule for deletion of scanned EOI documents. In addition igovt IVS full service should be designed in a way to make it possible to delete scanned documents in the future should automated means of checking EOI documents become available. This could include offering Service Users the option of undergoing a process that will remove the need to store their scanned EOI documents and enable them to be deleted from the igovt IVS.

Recommendation 13 – Business as usual: Reporting

IIS recommends that there should be a process for assessing what reports are and are not necessary for ensuring the proper operation of the igovt IVS and flowing from this, rules about what reports relating to the operation of the igovt IVS are, and are not, allowed and in what circumstances. DIA should establish a change and governance procedure to ensure that changes to the types of reports conducted are assessed to ensure they are only generated for purposes consistent with the igovt IVS.

Recommendation 14 – Business as usual: Assess in detail notification of igovt ID status

IIS recommends that DIA develop a guideline which outlines the basis on which it will exercise its discretion under Clause 20(2) of the EIV Bill to provide information about a change in status of an igovt ID to an agency participating in the igovt IVS. The guideline should ensure that DIA only exercises this discretion when it is necessary for a purpose that is directly related to the purposes of the igovt IVS. DIA should consult with the Privacy Commissioner in developing the guideline.

Recommendation 15 – Safety-net: Review of inquiries and complaints handling processes

IIS recommends that DIA reviews its inquiries and complaints handling processes to assess whether they are sufficiently coordinated and responsive to handle the increase in number and complexity of inquiries and complaints that will occur with the igovt IVS full service build and the addition of NZ Post as a partner. DIA should ensure that it discusses in detail the processes to be followed by NZ Post to ensure that the increase in integration at the process and the technology level is accompanied by a smooth, one-stop-shop integration at the human and customer service level. DIA should ensure it collects data about complaints processes (internally and from Users) and regularly reviews it for continuous improvement in its processes.

2 INTRODUCTION

The Department of Internal Affairs (DIA) has asked Information Integrity Solutions (IIS) to conduct a Privacy Impact Assessment (PIA) on the full service build of the igovt Identity Verification Service (igovt IVS). IIS conducted a PIA on the igovt IVS initial implementation phase in December 2009. DIA also asked IIS to conduct an assessment of privacy risks of the extension of the use of igovt services to the private sector and to New Zealand Post Group which is a State Owned Enterprise.

The igovt IVS is a key enabler of the New Zealand government's Result 10, ensuring New Zealanders can complete their transactions with government easily in a digital environment.

The igovt IVS Full Service build project has been initiated to deliver the full igovt IVS service offering. This includes meeting the legislative requirements in the Electronic Identity Verification (EIV) Bill.[1] This Bill was introduced to Parliament in August 2011, passed the first reading on Tuesday 12 February 2012, was reported on to Parliament by the Government Administration Committee on 12 June 2012 and has reached the second reading on 29 August 2012. The project also includes meeting DIA obligations under its partnering agreement with New Zealand Post Limited (NZ Post).

3 SCOPE OF PIA WORK

DIA asked IIS to conduct a PIA of the proposed enhancements to the igovt IVS including use of immigration and birth data and the use of NZ Post for the photograph and capture stage to ensure the service build is compliant with the Privacy Act.

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

The PIA also provides a privacy assessment of the extension of use of igovt services to the private sector. This will occur, for example, through the use of the igovt logon service by the provider of the Common Web Services platform to NZ government agencies. It will also take place, once the EIV Bill is enacted and enabling regulations provided for in the Bill have been promulgated, through the RealMe service being developed in partnership with NZ Post that will leverage existing igovt services. RealMe is the official digital verification and authentication service that enables individuals to access, manage and present their identity and personal information when interacting with NZ enterprises and government agencies online.

The PIA provides a general assessment of this kind of extension of use and makes an assessment of use of the igovt logon service by the Common Web Services platform. However, it does not make a detailed assessment of RealMe at this stage as DIA is proposing to conduct a detailed PIA on this in the near future.

[1] The Bill referred to in the PIA is the 12 June Version as proposed to be amended by the Government Administration Committee.

4 METHODOLOGY

IIS took the following steps for the PIA.

4.1 CONSULTED WITH DIA AND FINALISED WORK PLAN

In this phase, IIS met with the relevant people in DIA to discuss the project approach and then developed a project plan to deliver the work.

4.2 GATHERED INFORMATION

In this phase, IIS gathered and read information about igovt IVS full service build including:

- High Level Business Process models for the igovt IVS Full Service;
- Product Requirements Specifications for:
    - Apply;
    - Photo Capture;
    - DoL Verification;
    - Application details verifications and Image Determination;
    - Managing igovt IDs;
    - Death Matching;
    - Linking source identities through VIS interface;
- igovt IVS privacy risk register.

IIS also reviewed the partnering agreement between DIA and NZ Post.

4.3 STAKEHOLDER INTERVIEWS

IIS met with key stakeholders including:

- DIA staff;
- NZ Post;
- the Privacy Commissioner.

4.4 ANALYSIS

IIS developed a description and map of information flows and identified any privacy risks taking into account the Information Privacy Principles (IPPs) in the *Privacy Act 1993* and other privacy risks that could arise that go beyond non-compliance with the law.

4.5 PREPARED DRAFT REPORTS AND DIA REVIEW

Once analysis and consultation was completed, IIS prepared draft reports which included draft recommendations. IIS provided the drafts to DIA for comment. Drafts also took into account updates in the progress of the EIV Bill and some additional assessments DIA requested.

4.6 WROTE FINAL REPORT

IIS then wrote the final report taking into account the feedback from the DIA.

5 ASSUMPTIONS

IIS assumes that the reader of this report has some familiarity with the igovt IVS and how it operates. A fuller description of the initial implementation of the igovt IVS can be found in the PIA IIS prepared on the initial implementation.

IIS also assumes that its focus in this report should be on the key risks that it has identified and deserve discussion rather than describing in detail every risk it has looked for and found to be addressed.

6 LIST OF TERMS

Term	Explanation
BDM.	DIA Births, Deaths and Marriages
DIA	Department of Internal Affairs
DoL	Department of Labour – In the context of this document DIA this is specifically interaction with NZ Immigration.
EIV Bill	Electronic Identity Verification Bill – Describes the requirements intended to be enacted for the administration and operation of the Electronic Identity Verification Service (i.e. igovt IVS). The Bill's contents are subject to change through the legislative process. The Bill referred to in the PIA is the June 12 Version as proposed to be amended by the Government Administration Committee.
EOI	Evidence of Identity – The types of evidence that when combined provide confidence that an individual is who they say they are
EOI Source Agency System	Currently NZ Passports and NZ Citizenship For igovt identity purposes, specific Identity information for an individual (e.g. name, date of birth, place of birth and gender) is deemed to have been sufficiently established, validated and stored by several authoritative source systems: Passport System and Citizenship system.
Federated identity	Federated Identity refers to a grouping of identity numbers for the same person. The information is grouped in such a way that only the identity number will be returned to the calling application which the calling application had created in the first place.
FID	Federated Identifier – an identifier that maps to a person

	identifier in an identity source system. In diagrams this could be called the PFID (passports), CFID (citizenship), IFID (immigration), BFID (birth).
FIS	The Federated Identity Service (FIS) queries the FID database and returns a federated identifier (FID) for igovt IVS which is mapped to a given EOI Source Agency System Identity ID (Person ID) (e.g. Passport person or a Citizenship person, and, in the full igovt IVS build will map to person identifiers for Department of Labour and Births Deaths and Marriages.
igovt ID	The electronic combination of 4 types of identity attributes that have been verified and held together to make up a unique core identity combination for an individual; made up of customer's full name, date of birth, place of birth and gender.
igovt IVS	igovt Identity Verification Service – An all-of-government shared service that provides individuals with the option to verify their identity authoritatively, online, and in real-time with participating agencies to a passport level of confidence.
igovt logon service	The igovt logon service allows Users to use the same logon details to access all participating government service provider's online services. This saves Users from having to remember multiple logon details for different services. A logon is required to be specified as part of the creation of an igovt ID.
Moderate strength (igovt) logon	The logon strength required for moderate service risk transactions. Requires a username and an authentication key that is at least one of the following: a one-time password system combined with a password; a one-time password device requiring per-session local activation (with a password or biometric) or a software token requiring per-session local activation (with a password or biometric).
RealMe	RealMe is the consolidated name for the services previously branded as igovt within the New Zealand public sector. These service offerings have now been extended to provide authentication and identity attribute assertion services for the private sector.
Real-time	Relating to a system in which input data is processed within milliseconds so that it is available virtually immediately as feedback to the process from which it is coming.
Person ID, PID	This is the identifier assigned by a particular agency, such as a passport record number, citizenship record number, immigration record number, or birth record number. In diagrams these may be called PPID,CPID, IPID, BPID
Service Agency (SA)	An agency (public or private) who provides a service or services to customers
VISI	Verified Identity Source Interface – Technical means for accessing

	EOI data within the DIA domain.

7 GENERAL DESCRIPTION OF THE IGOVT IVS

The igovt IVS is intended to be an all-of-government shared service. It is 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 gender. These four verified key attributes make up the igovt ID. The igovt ID is an electronic credential that the User can assert to government agencies to verify their identity in an online environment.

The igovt IVS establishes identity as part of the igovt suite of services. The other key part of the igovt services is the igovt logon service. The igovt logon service is an all of government shared service to manage the logon process for online services of participating agencies. The logon service can assure the Service Agency that a Service User using a validated Federated Logon Tag (FLT) is the same Service User who used the validated 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 igovt IVS provides functions that the logon service cannot provide. The igovt IVS adds the concept of absolute identity to the services available to a Service Agency. The igovt IVS seeks to verify that the identity being asserted to a Service Agency is unique. In addition, if asked to do so, the igovt IVS can provide the external attributes of name, date of birth, gender and place of birth.

The igovt IVS is treated as a Service Agency in relation to the igovt logon service. The Service User will be transferred to the igovt logon service to log on, then back to the igovt IVS.

A key design feature of the igovt IVS has been to keep the information the igovt IVS collects to verify identity separate from the information the igovt logon service holds to provide logon services. The igovt logon service is operated by Datacom, while the igovt IVS is operated by DIA and both are housed at Datacom.

The stated objectives of the igovt 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 has tested the concept of the igovt IVS through an initial implementation of a limited form of the igovt IVS enabling people with an igovt ID to order certificates and printouts from Births, Deaths and Marriages.

The initial implementation of the igovt IVS uses Evidence of Identity (EOI) source records from New Zealand Passports and Citizenship to issue the igovt ID to users. To gain an igovt ID the individual needs to have a valid passport issued, or been granted citizenship, since 1 January 2004.

The set of attributes to be provided by the igovt IVS to the Service Agency is 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 igovt IVS.

The igovt IVS uses the current databases of passport and citizenship information for EOI purposes. These are cross-referenced via the Verified Identity Source Interface (VISI) so that the igovt IVS can ensure that one individual does not create two identities, one based on each eligible EOI source type (passport and citizenship).

Stages in the process for issuing an igovt ID are:

- Apply for igovt ID;
- Photo capture;
- Create igovt ID (which in the full service build includes Department of Labour (DoL) verification, information and document verification, and image determination.)

Once the person has been issued with an igovt ID they are able to:

- Use (assert) their igovt ID;
- View their igovt ID activity;
- Cancel their igovt ID.

In the initial implementation of the igovt IVS, applications could only be made at a mobile office or at some DIA offices. Since the PIA on the initial implementation, the igovt IVS was enhanced to enable individuals to apply online from any computer with access to the internet. However, once the initial application process is completed, the User must physically go to an equipped DIA customer service office for the photo capture stage.

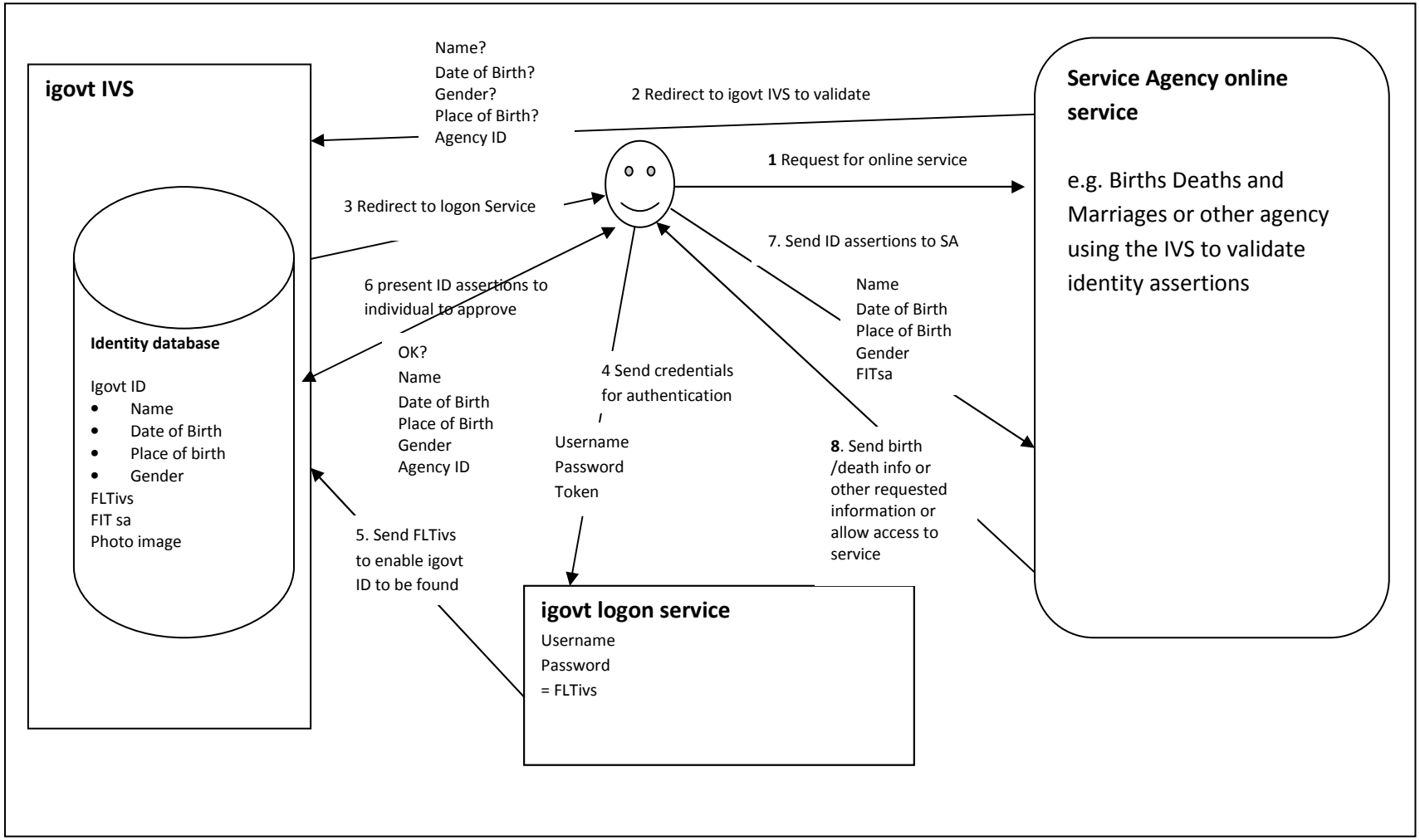
An applicant must have a moderate strength igovt logon for the initial online application stage and for subsequent assertions of identity using their igovt ID. If a person does not have a moderate strength igovt logon then an additional first part of the application process will be to set up a moderate strength logon.

To gain a moderate strength logon the applicant must provide a mobile phone number in order to receive a one-time password by TXT to enter in addition to their igovt logon username and password. A person can also be issued with a one-time password token.

At various points in the application process for an igovt ID, applicants are notified of how their application is proceeding, that they may need to bring more information, of what to do next, and the outcome. In each case, email information is obtained through the igovt logon service.

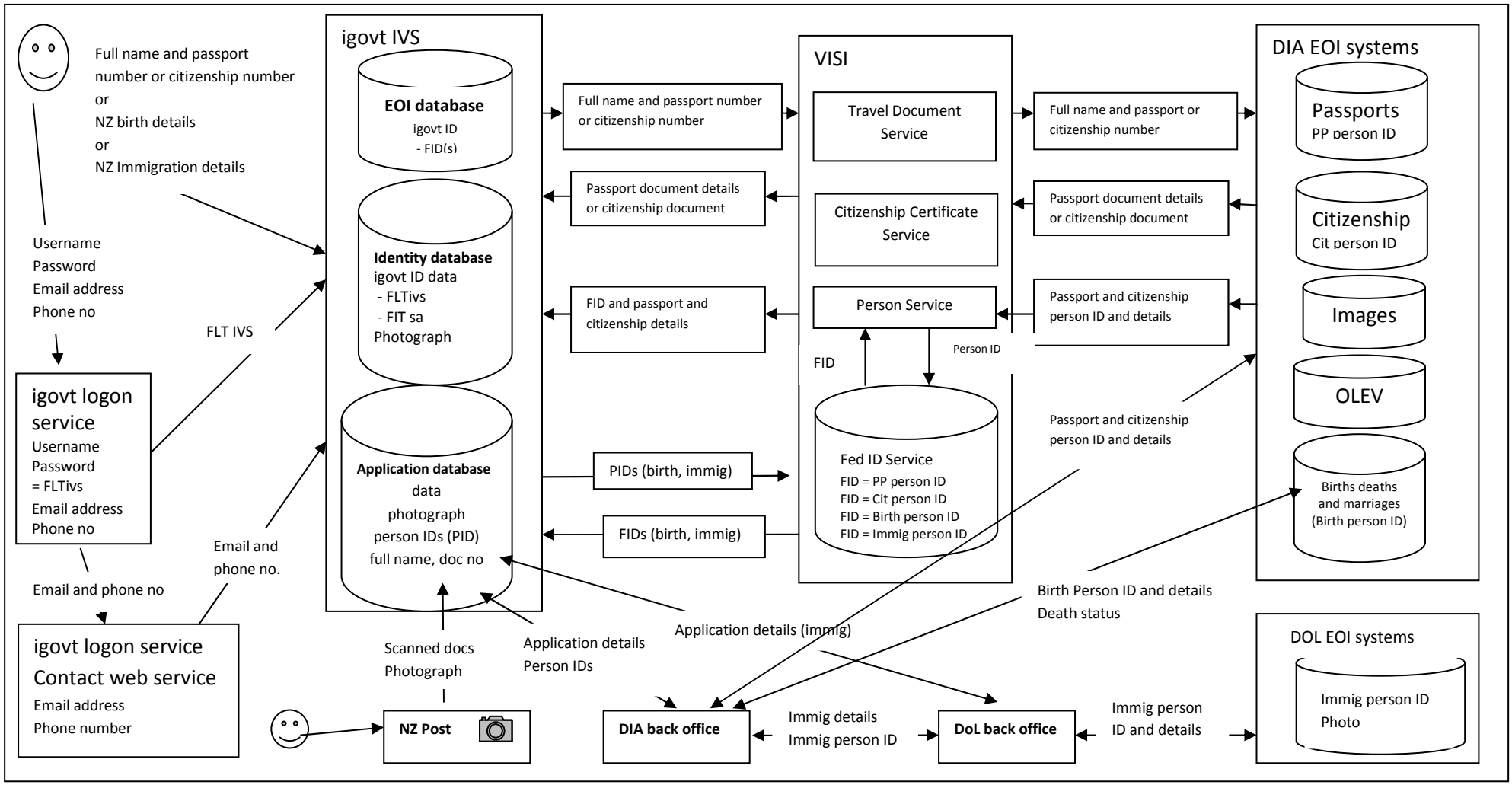
The following is a diagram in 7.1 which describes the information flows for the Use (assert identity) stage which will remain current through the igovt IVS full service build. In 7.2 the diagram describes where data is stored and the information flows during the igovt ID application process.

7.1 ASSERT IDENTITY INFORMATION FLOW DIAGRAM



7.2 INFORMATION FLOWS

The following is a general indication of the data holdings and flows in the igovt IVS full service build taking into account all the bases on which an application for an igovt ID might be made. Note that the person IDs are deleted from the igovt IVS applications database once the uniqueness process is completed.



8 CHANGES FOR IGOVT IVS FULL SERVICE BUILD

8.1 NATURE OF AND REASON FOR KEY CHANGES

The full igovt IVS build will be subject to the requirements of the EIV Bill. Once the EIV Bill is in effect, private sector and agency use of the igovt IVS will require a Cabinet decision and to be authorised in regulations under the Bill.

Changes to the igovt IVS for the full service build are also designed to ensure compliance with the EIV Bill. Many of the changes are a result of the EIV bill expanding the range of people in New Zealand who can apply for an igovt ID. This has added significantly to the complexity of the Evidence of Identity (EOI) process because many people in the expanded categories will not be in a position to rely on highly authoritative EOI sources such as a New Zealand passport or citizenship certificate issued after 1 January 2004. To maintain the integrity of the igovt ID as a high strength assertion of identity applicants will be required to provide physical copies of a range of sources of EOI based on an applicant's age (only applicable for applicants of all ages using NZ Immigration and NZ Birth details), immigration status, birth being in New Zealand, and name change (only if change registered overseas). At this stage of the igovt IVS full service build much of the verification for these additional sources of EOI will need to be done manually using back room processes rather the more fully automated online processes available for passports and citizenship certificates issued after 1 January 2004.

The EIV Bill will allow partnerships with the private sector and DIA has now partnered with NZ Post to support the issuing of igovt IDs and to enable NZ Post to provide private assertion services. The igovt IVS full service build will include changes to enable NZ Post to provide the photo capture part of the igovt ID application process in addition to DIA.

DIA is working with NZ Post to provide a service called RealMe which integrates the igovt IVS and igovt logon service with other NZ Post services and to make them available to the private sector as 'participating agencies' (in the same way as government agencies currently participate) and their customers.

The following sections outline in more detail the business and system changes being made for the igovt IVS full service build.

8.2 EXTENDS ELIGIBILITY TO APPLY FOR IGOVT ID

A key change is that the range of people able to apply for an igovt ID will be significantly extended beyond those who have been granted citizenship and those with a passport issued after 1 January 2004. igovt ID issuance will now be available to all people in New Zealand including:

- people born in New Zealand who do not have a NZ Passport issued since 1 January 2004;
- immigrants with details verified against immigration data (such as a Visa, proof of Australian citizenship);

- Children under 16 and also to those under 14 years who have Parental / Guardian consent[2].

8.3 EXTENDS AUTHORITATIVE SOURCES OF EVIDENCE OF IDENTITY INFORMATION

In the current implementation, Passports and Citizenship records are the only authoritative sources of evidence of identity that can be used to verify an applicant's identity. The igovt IVS system can check these records in real-time online and will continue to do so in the full igovt IVS service build.

The igovt IVS full service build will draw upon a wider range of authoritative sources of EOI information. These sources will now include immigration data and birth record. The full build will include a wider range of passports. An expired passport issued since 1 January 2004, in addition to current passports issued since 1 January 2004, will be regarded as valid evidence of identity and the applicant will not need to produce it physically to proceed with the application. [redacted]

[redacted]

Withheld to prevent improper gain or advantage

8.4 CHANGES TO APPLICATION PROCESS

The application stage process online is broadly similar to the one used in the limited service with the following changes:

- users are given more options for choosing the EOI source they wish to apply on the basis of;
- a screen specific to the EOI source they choose is displayed to be completed which, depending on the nominated source, may require the User to enter relevant identity attribute details and document details;
- users are given the opportunity to provide their new name details if details on EOI documents or birth name are no longer current;
- users receive an application number (by email and text) which they take with them when they attend in person at DIA or (in another change) an NZ Post outlet for the photo capture stage and are notified of next steps including to bring application number and the documents they need to bring to establish their identity;
- users are asked to provide their consent to the photo capture process;
- the photo capture operator uses the application number to locate the person's online application (currently this search is done using the EOI document number).

8.5 CHANGES TO PHOTO CAPTURE STAGE

Once a person has completed the initial application phase they must physically attend a DIA office or NZ Post outlet to have their photograph, and documents (if applicable) digitally captured. In the initial igovt IVS implementation, this would also be the point at which the photo returned from Citizenship or Passports is compared with the captured photograph to ensure that the person relying on the EOI source is the person to whom the EOI document was issued (photo validation). However, as a result of limited service build enhancements currently operating this photograph validation

[2] See Clause 7, Electronic Identity Verification Bill, definition of 'Applicant'.

phase has been separated from the photo capture phase and is now an igovt IVS back office function.

Under the igovt IVS limited service build the applicant must log in to the igovt IVS via the igovt logon service using a moderate strength logon at the photo capture stage.

Under the igovt IVS full service build NZ Post will be a major provider for the photo capture stage of the igovt ID issuance process. Operators will retrieve a person's igovt ID application from the igovt IVS system through a search on the application number. They will also upload the applicant's digitally captured photograph and documents (if applicable).

Steps in this phase that have changed as specified in the initial requirements include:

- the applicant must provide an application number to enable the photo capture operator to retrieve the applicant's igovt ID application;
- the operator asks the applicant to consent to having their photograph taken, and the operator must indicate that the applicant has consented, otherwise the applicant is unable to complete the photo capture stage;
- the operator asks the applicant to confirm the full name he or she used to complete the apply stage in order to link the applicant to the correct application;
- if the applicant is under 14, the photo capture operator must indicate that they have sighted the applicant's parent or guardian, otherwise the applicant is unable to complete the photo capture stage;
- the operator asks the applicant to present all the EOI documents (in original and translations if applicable) they must provide as listed on the person's igovt ID application depending on whether they:
    - are relying on:
        - NZ birth details; or
        - NZ immigration details;

        in which case they must provide a source document that has their photograph on it, or if that is not possible, then other photo ID such as a photograph on a driver licence;
    - are a child under 14 years applying on the basis of NZ Immigration or NZ Birth details (e.g. proof of parentage, guardianship, proof of name change of parent, guardian, consent form);
    - seeking to have their igovt ID in a name different from that on their EOI documents or birth name, in which case, if their name change is registered overseas, they must provide proof of name change from the overseas registration source;

- the operator scans the documents and photo ID and uploads them into the igovt ID application;
- the operator indicates on the application that the photograph and photo ID (if applicable) is of the applicant;
- where immigration data is relied on the igovt IVS sends an email to the DoL to notify them that an application based on NZ immigration details requires verification;
- it will be a requirement that the photograph or other scanned documents are deleted from NZ Post system once the upload is completed. However, this will take place outside the igovt IVS system and is not under igovt IVS control.

An applicant relying on Citizenship certificate or current or expired NZ Passport issued after 1 January 2004 will not be required to produce these documents at the photo capture stage unless they are under the age of 14.

8.6 CHANGES TO PROCESS FOR VERIFYING DATA

In this release of the igovt IVS full service build it will not be possible to verify NZ immigration data or NZ birth records online in real-time. DoL is in the process of rebuilding its data systems to enable this, but this will not be complete for several years. As a result, many of the steps in the identity verification process will be back office business processes which will involve, for applications based on immigration, manual back office details verification by DoL staff. It will also involve igovt IVS back office activity for a number of other business processes.

There may also need to be phone or email discussions between DIA and DoL in the course of the verification process.

At data verification stage of the application process, DIA and DoL staff will be able to logon to the igovt IVS system via the igovt logon service using a moderate strength logon.

To verify immigration data at this stage the DoL operator will:

- search for the relevant application to be verified using the application number emailed to them from the photo capture process, or searching for applications based on DoL verification business process state;
- check that the application details provided match those of the immigration EOI source, e.g. visa, or Australian;
- the operator also checks the photo captured during the photo capture process and indicates whether or not the photo matches the photo image held by DoL, or otherwise indicate that DoL does not have a photo. (However, this does not replace the photo determination stage conducted by DIA later in the process.);
- the operator may need to contact DIA to discuss what to do in circumstances where details do not match and to keep note of the outcome of such discussion.

The igovt IVS back office will also need to undertake verification steps. For example, where:

- the applicant is a child under 14 and has not provided the relevant parental or guardian consents or verification details;
- there has been a name change indicated in the apply stage;
- there has been no photograph supplied from the EOI source system.

In these cases, the igovt IVS operator will:

- make sure that the applicant has provided all the necessary documents and then scan them in. In some cases, this may include the photo on a drivers licence or a foreign passport;
- in the case of reliance for EOI on expired NZ Passports, NZ birth details and NZ immigration details verify if a death record is held with Births, Deaths and Marriages. [redacted] Withheld to prevent improper gain or advantage
- in other cases take the necessary steps including contacting the appropriate authoritative source or third party (which may be overseas) to verify that the identity is living, that the person giving consent to the child gaining an igovt ID is the child's parent or guardian and to verify documents.

The igovt IVS back office operator and the igovt IVS system also take a number of steps to ensure that the person has not previously been issued with an igovt ID and cannot be issued with another one at any stage based on the other available authoritative sources of EOI. This is called establishing uniqueness.

This includes:

- the operator checking if the applicant's identity details exist in the other authoritative EOI source systems, and retrieving the EOI source system unique Person ID (obtained from either NZ Immigration or NZ Birth), and or person details (full name and document number – from either NZ Passport or NZ Citizenship), and inputs it into the igovt ID application in order for the igovt IVS to do the uniqueness checking;
- the igovt IVS automatically sends the Person ID(s), and or person details and document number to the VISI;
- the igovt IVS stores the NZ Immigration visa or permit number into the Application database (in the igovt IVS system) for applications made using NZ immigration details;
- the Federated Identity Service in the VISI:
    - will check if there is a FID that is associated with the Person ID (obtained from either NZ Birth or Immigration) and if it exists then sends it to igovt IVS and if it doesn't exist then it generates a FID for the Person ID stores it in the Federated Identity Service (FIS) of the VISI, and sends it to the igovt IVS; and

- uses the person details (full name and document number) to check if the applicant's identity exists in either of the NZ Passport or NZ Citizenship systems. If the identity does exist the person ID will be used to check if there is a FID that is associated with it. If it exists it is sent to the igovt IVS, and if doesn't exist then it generates a FID for the unique person ID record and stores it in the Federated Identity Service (FIS) and sends it to the igovt IVS;

- The igovt IVS automatically discards the Person ID(s), and or person details and document number that had been inputted into the application by the operator, when the FID(s) are received from the VISI;

- the igovt IVS will store all FID(s) received from the VISI into the EOI database, except at the verification stage of application process where it finds that a FID (of a particular type) from the VISI is not the same as the FID of (that particular type) already stored in there for that person. This could arise where a person is renewing their igovt ID using the same EOI they used the first time they applied for an igovt ID.

[redacted]
Withheld to prevent improper gain or advantage
[redacted]

In some cases the igovt IVS operator may need to contact the child applicant's parents, amend an application, or decline an application if the documents provided cannot be verified.

Image determination is the last step taken before an igovt ID is created. This process is the same as that provided for in the initial implementation, except that the photos used to compare with the captured photograph may come from a scanned driver license, HANZ 18 card, firearms licence, or overseas passport photograph, for those applications where the photograph could not be obtained from the authoritative EOI source (i.e. NZ Immigration and NZ Birth). As with the initial implementation, the images retrieved from the source agency or scanned photograph must be discarded once the image determination is complete. However, where a licence has been scanned, the whole licence image is retained, including the photograph.

A future release of the igovt IVS full service build is proposed to include one-to-one facial recognition for the purpose of assisting with the image determination phase (currently done through human visual analysis).

8.7 Enables Service User to update their igovt ID attributes

The igovt IVS full build will enable a Service User to logon to the igovt homepage and request a change of name (but not other igovt ID attributes) using the 'Manage igovt ID' screen. The need for this may arise, for example, due to adoption, registered name change or gender change. Unless the name change can be verified through the igovt IVS back office matching information with relevant DIA business groups, the Service User will be asked to provide original documentary proof which must also be checked. In the initial implementation, a Service User would have had to cancel their original igovt ID and apply for a new one. Attribute changes other than to name will require use of other channels (yet to be determined). Changes to name or other attributes requested due to errors

in source documents will require the User to go back to the source and have the original documentation amended before proceeding with the update of an attribute.

8.8 Provides for a Service User and participating agency to be notified of a change of igovt ID status

The EIV Bill has provisions governing the cancellation, suspension or revocation of an individual's igovt ID by the chief executive including giving the individual the right to make submissions about a decision (Clauses 28-32).

The igovt IVS full service build will provide for the igovt IVS to manually notify the User and relevant participating agency or agencies:

- if a User's igovt ID status is changed to:
    - suspended;
    - deceased;
    - revoked;
    - withdrawn;
- of the outcome of a User requested igovt IVS back office review of a decision DIA has made about the status of a User's igovt ID.

8.9 Increases reporting functionality to enable Privacy Commissioner to ask for reports

Clause 53 of the EIV Bill[3] provides that the Privacy Commissioner may require reports to be made on a range of matters relating to the igovt IVS. The igovt IVS full service build reporting functionality will be enhanced to ensure that it can report on the full range of matters outlined in the Bill. These matters are:

- the operation of the igovt IVS or any aspect of it including:
    - the number of participating agencies;
    - the number of igovt IDs that have been issued or cancelled;
    - the types of transactions or services for which igovt ID are used;
    - the number of times igovt IDs have been used by all or any classes of individuals;
    - the number of times that persons have accessed individuals' records of usage history for purposes specified in the Bill;
    - any issues that have arisen, or that are likely to arise, in the use of the igovt IVS.
- the operation of a confirmation agreement entered into in accordance with Schedule 1 which regulates the identity information verification (checking) part of the igovt ID application and issuance process.

[3] 12 June 2012 Version as proposed to be amended by the Government Administration Committee.

8.10 Enables NZ Post to provide igovt IVS related services to individuals and the private sector

As authorised by Clause 47 of the EIV Bill, DIA has entered into an agreement with NZ Post Limited to enable NZ Post to provide a service called RealMe which is intended to make igovt IVS and the igovt logon service more easily accessible to individuals.

RealMe is to be the official digital verification and authentication service that enables individuals to access, manage and present their identity and personal information when interacting with NZ enterprises and government agencies online. It seeks to enable individuals to interact conveniently and securely online with the confidence that they are in full control of their identity and personal information. The RealMe business model is a consolidated arrangement for public and private sectors, incorporating the igovt logon service and using both the igovt IVS and NZ Post's address verification service.

The combination of the igovt IVS and address verification service is believed to be of interest to banks which will be subject to anti-money laundering and countering financing of terrorism legislation in early 2013.[4]

9 ASSESSMENT OF RISKS OF EXTENSION OF IGOVT SERVICES TO THE PRIVATE SECTOR, NZ POST AND WEB SERVICES PLATFORM

9.1 Introduction – potential risks

In many ways the same or very similar privacy risks are likely to arise from extension of use of igovt services to the private sector or to quasi-private sector organisations such as NZ Post, as arise with the addition of new public sector organisations to use of igovt services. It cannot be assumed that private sector organisations are necessarily less likely to respect the privacy of individuals than public sector organisations. Both types of organisations must comply with the Privacy Act.

The following sections consider the general risks that could arise in relation to igovt services and considers whether there are particular issues that could arise from extending igovt services to the private sector or NZ Post. This section is not a PIA on RealMe. DIA has commissioned a detailed PIA on the RealMe initiative.

9.2 General risks and applicability to private sector

9.2.1 Tracking the lives of individuals

A key risk in identity related initiatives is that the organisations involved might gain an increasingly rich picture of the lives of individuals. This could potentially be used for new or unrelated purposes. Rather than deriving from the content of interactions, this picture is likely to derive from the dynamic data and audit logs that result from those interactions. This could enable a picture of such matters as who the individual is interacting with, at what times, what dates and for how long.

As private sector organisations are allowed to use igovt services new aspects of a person's life are added to the mix. Generally, a person has more interactions with some private sector organisations

[4] http://www.dia.govt.nz/Anti-money-laundering-and-countering-financing-of-terrorism

(for example, banks) than with government organisations and so there is increased scope for gathering data about a person's life.

It is increasingly being recognised that "[D]ata grows ever more connected and valuable with use. Connecting two pieces of data creates another piece of data and with it new potential opportunities (as well as new potential harms)".[5]

In the case of the igovt logon service on its own, the addition of more organisations, public or private sector appears to be generally a lower privacy risk because it does not store highly identifiable information about individuals logging on. Although the igovt logon service keeps logs of interactions, in most cases it will not have enough data to be able to connect the logs to an identifiable individual.

In the case of the igovt IVS, the tracking risks associated with of logs of interactions is much higher because it does hold identifying information about igovt ID holders. The logs will be increasingly rich as more organisations (public or private sector) are able to use the igovt IVS as participating agencies. The government has significantly mitigated these risks through the EIV Bill which places significant restrictions on access to, and use and disclosure of, transaction history held within the igovt IVS.

Depending on how it is designed, the addition of NZ Post and its RealMe service could create further complexity and richness. As integrator of igovt and other services depending on the design there may be significant potential for RealMe to collect logs not just about individuals' igovt related interactions but also about other services it provides to the individual. These kinds of issues can be explored in a new PIA which IIS understands DIA is to commission soon.

9.2.2 Reduced choice

As more organisations use igovt services and those organisations include private sector organisations there is a risk that the privacy protections provided by choice, such as whether to use igovt services at all, lose their power. Society as a whole may become increasingly reliant on these channels for government and non-government interactions. Other options may be increasingly discouraged and possibly even become unavailable. In these circumstances, individuals may not be in a position to take the protective option of withdrawing from use of igovt services if they find that unwelcome function creep is occurring or they otherwise lose trust in the system. Although not strictly a privacy issue, some sections of the community that are unable to afford the costs of online interaction could become further marginalised.

9.2.3 Complexity leading to less transparency

As more organisations use igovt services as participating agencies and the wider the range of uses, such as those of NZ Post, the more difficult it could become to be transparent to individuals about information flows and the information handling roles. This arises in relation to both public sector and private sector organisations. Attempts to achieve transparency through long privacy notices will be increasingly less appropriate. Providing access to information about the content of transactions as well as the logs will also be essential, but become more complex. Some private sector

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

organisations may be less accustomed to designing their systems in a transparent way and in a way that enables individuals easy access to all personal information about them held, including logs.

9.2.4 WEAKENED OR INCONSISTENT APPROACH TO SECURITY AND PRIVACY

Ensuring a consistent and robust approach to security when private sector organisations are added as users of igovt services may become more difficult. Private sector organisations are not subject to the government wide guidelines and protocols around security, such as the New Zealand Information Security Manual, which apply in the public sector. As a result, there is a risk that the robust security provisions applying to igovt services could be compromised by weak security in one or more private sector users.

Although this issue can be managed through strong contractual terms there is a risk that terms could become inconsistent with each new user and over time. This could result in a complex privacy and security regime that is hard to administer, monitor and enforce. IIS notes that the igovt partnering agreement with NZ Post includes a set of "compulsory terms" for its integration agreements with private sector entities. These include privacy and security provisions.

9.2.5 BURDEN OF RISK AND LACK OF SAFETY-NET

With the introduction of more participants in igovt services there is a risk that when privacy or security failures occur there is no entity with clear responsibility for receiving inquiries or complaints and then to ensure that an inquiry or complaint is resolved to the satisfaction of the individual. There is a risk that the individual could be left to approach a number of different organisations to have their inquiry or complaint resolved and potentially no one organisation willing to accept responsibility. This issue arises whether private or public sector organisations are involved.

9.2.6 FUNCTION CREEP

There is a risk that, for commercial or other reasons, the terms on which private sector organisations are allowed to use igovt services could change over time without any assessment of the privacy implications of such changes. However, function creep is an issue for both public and private sector users.

9.3 RISK ARISING FROM IMPACT OF BUSINESS AND GOVERNMENT IMPERATIVES

IIS considers that a key risk arising from involving private sector or quasi- private sector organisations in use of igovt services is that the general igovt commitment to privacy could be weakened as a result of:

- government incentives to reduce costs, or raise revenue, through either selling igovt services to the private sector or in allowing private sector or NZ Post to provide, or help provide igovt related services; and
- business imperative to make a profit out of using igovt services or of helping to provide igovt related services.

A combination of these factors could drive decisions, without proper public scrutiny, about use of igovt services and the terms of such use, that give privacy a lower priority than might otherwise have been the case. Where individuals have a choice about whether or not to use igovt services this may

not create major privacy issues although it may result in wasted resources due to lack of individual take up.

However, where individuals are compelled to use igovt services for legal, practical or other reasons, there could be significant privacy risks for individuals, including the ones raised above.

9.4 INITIAL ASSESSMENT – GENERAL

IIS considers that extension of use of igovt services, particularly the igovt IVS, to the private sector and quasi-private sector such as NZ Post could raise privacy risks due to:

- the fact of general increase in numbers of organisations using igovt services;
- the range of individual life activities and associated activities that can be added to meta data and audit logs;
- the increase in complexity of organisational arrangements leading to less transparency and clear avenues of responsibility for inquiries and complaints;
- lack of clarity about, and complexity of, governance arrangements between government and the private sector organisations involved, which could lead to security weaknesses, and decisions which give less priority to privacy without proper public scrutiny and accountability.

Many of the privacy issues can be dealt with on a case by case basis taking into account the fact that DIA has a strong record in conducting PIAs with each incremental change.

However, IIS considers that the key risks arising from extension of use of igovt services to the private sector will not be addressed unless there is a comprehensive, accountable and clear privacy governance mechanism that provides ongoing oversight of igovt services as they develop into the future and is embedded in wider igovt governance and decision-making processes.

This privacy governance process will also ensure that igovt initiatives are not developed in isolation without any big picture view of the privacy risks when they all come together. This governance structure should enable:

- end-to-end oversight of all igovt initiatives;
- the development of consistent lines of accountability for privacy;
- coherent policies and requirements relating to the management and implementation of privacy for all igovt service users including the terms and conditions of integration with igovt services;
- monitoring mechanisms for all participants;
- coherent and accountable processes for managing change and dealing with function creep;
- involvement of the community and the private sector in key decisions.

The need for this coherent governance structure is becoming more urgent as there are an increasing number of proposals for private sector organisations to use igovt services.

Recommendation 1 – Independent and coherent governance structure for use of igovt services
IIS recommends that as a matter of priority DIA develops a coherent governance structure for managing the administration and evolution of igovt services and their use by public sector, quasi private sector, and private sector organisations. The governance structure should include a mechanism for community and private sector stakeholders to participate in decision making about use of igovt services and the terms and conditions of such use. The roles and functions for the governance structure should include:

- a person responsible for oversight of end-to-end and big picture privacy issues as igovt services evolve and become accessible to a wider range of users;
- development of coherent policies and requirements relating to the management and implementation of privacy for all igovt service users;
- oversight of the terms and conditions on which new organisations integrate to ensure that the current high standard of security and privacy requirements are maintained and implemented in a consistent way;
- the establishment and implementation of mechanisms to monitor compliance with the policies and requirements by all users of igovt services;
- the development and implementation of formal and coherent and accountable processes for managing change and dealing with function creep;
- establishing an ongoing mechanism for involving of the community and the private sector in decisions about the evolution of use of igovt services.

9.5 Assessment – Common Web Services Platform

9.5.1 Common Web Services Platform

One proposed extension of igovt services arises from DIA's intention to integrate its proposed Common Web Service Platform for NZ government agencies with the igovt logon service.

DIA has issued an RFP for providers of a Common Web Services Platform. This project will involve a single private sector supplier implementing and hosting a shared content management system. The Government intends to leverage IaaS as its preferred infrastructure foundation for this platform. The single supplier will establish a repository for shared code and templates which will be available to anyone across government.

DIA is proposing that users of the Common Web Service Platform would use the igovt logon service for web user authentication, including for Agency content management functions.

9.5.2 Possible issues

IIS has assessed the privacy issues in the extension of igovt logon services to private sector organisations providing common IaaS services to government. In this case, public sector employees

use igovt logon service to authenticate themselves to the IaaS service portal website to perform various functions including access reports, procure IaaS services and change technical parameters.

IIS considers that access by government employees (or service provider employees) to the Common Web Service Platform using igovt logon service raises similar issues to those IIS identified in its PIA on to IaaS service provider use of the igovt logon service. This includes because the infrastructure for the Common Web Service Platform is likely to be provided by one of these IaaS service providers, in particular, Datacom.

IIS makes the following recommendation which is similar to those it made in its report *Privacy Assessment: Extension of igovt logon service to Datacom and other private sector IaaS providers*.

Recommendation 2 – Common Web Service Provider use of igovt logon service
IIS recommends that:

- the Common Web Service provider is transparent about the fact that it is using the igovt logon service;
- where a Common Web Service provider using the igovt logon service also provides other identity related services to DIA, DIA ensures that the service provider has strict access controls in place that prevent any system administrator (or other person) from having a view of more than one of these services;government employees using the Common Web Service and igovt logon service have easy access to one-time-password tokens so that they can have more than one moderate strength logon if they choose to do so; and
- as identified strongly in the extension of igovt services to the private sector analysis, there are appropriate governance mechanisms to oversee terms and conditions for use of igovt services and to ensure the privacy impacts of change are assessed.

10 POSSIBLE ADDITIONAL PRIVACY RISKS RELATING TO IGOVT IVS FULL SERVICE BUILD

The privacy impacts of the igovt IVS have already been assessed in previous PIAs. This PIA will not revisit these risks. This section will consider whether the changes create additional risks. Key questions include whether involving NZ Post in the issuance process or as a partner in the proposed way creates new privacy risks or weakens the strong privacy underpinnings of the igovt IVS. The following table considers the privacy issues that could arise as a result of changes made for the igovt IVS full build. The section that follows this discusses in more detail any privacy issues that IIS considers should be discussed further.

Privacy Principle	**Possible risk**
Lawful purpose, collection necessary (1) Collection limitation	Risk that the igovt IVS, DoL, or NZ Post collects information about an applicant for a purpose that is not lawful or connected with its function or activity. Risk that DoL or NZ Post collect more information about igovt ID holders or applicants than they need to perform the role they play in

	the application process.
Direct collection (2)	Risk that manual identity checking processes (igovt IVS back office, DoL) could result in information about an applicant being collected indirectly without their knowledge or consent.
Notice/Transparency (3)	Risk that applicants will not understand the role of NZ Post in the application process.
Unfair, intrusive collection (4)	This is unlikely to become an issue in relation to these services.
Storage and security (5)	Risk that complex manual back office identity checking process could create significant security risks including unintentional or accidental breaches, intentional but unauthorised breaches, and malicious breaches. Risk that NZ Post data protection processes at the photo capture stage are less stringent than those of DIA offices Risk that DoL or NZ Post staff may get access to more information in the igovt IVS than they need to for their particular role creating a security risk. [redacted] Withheld to prevent improper gain or advantage [redacted] Risk that scanned EOI documents create a valuable 'honey pot' of identity documents which those with malicious intent such as identity theft devote considerable resources to get access to.
Access (6) Correction (7) (EIV Bill s 4(1)(e) and (f))	Risk that the igovt IVS will not be in a position to give an igovt ID holder access to their captured photograph or scanned documents stored with their igovt ID if an individual asks for such access.
Accuracy (8)	Risk that there could be more mistakes and inaccuracies in information held in the igovt IVS as a result of the complex manual checking processes.

Retention (9)	Risk that scanned photographs and other documents are kept in the igovt IVS for longer than they are needed for the purpose for which they were collected.
Limits on use (10)and disclosure (11) Function creep	Risk that documents scanned into and stored in the igovt IVS result in a richer store of information in the one place about an igovt IVS user and create greater incentive to use and disclose information in the igovt IVS for purposes unrelated to those of the igovt IVS. Risk that NZ Post might use or disclose information it collects at the photo capture stage of an igovt IVS application for purposes unrelated to the igovt IVS such as marketing or NZ Post commercial purposes.
Unique identifiers (12) and data matching EIV Bill s 36 (overrides rule 6 of the info matching rules in Sched 4 of Privacy Act.	Risk that a person's application number could become used as an identifier for matching purposes.
Choice and control	Risk that over time and as more agencies and private sector organisations use the igovt ID that use of the igovt ID will become the default, which will increasingly make it difficult for individuals to choose not to use an igovt ID as per Principle 1(a) in Clause 4 of EIV Bill.
Allocation of risk	Increased risk with expanded igovt IVS full service which includes NZ Post photo capture stage, that when mistakes or problems occur: • Individuals will have their igovt ID application refused, or their igovt ID suspended, cancelled or revoked with no avenue of redress, or no easily accessible avenue of redress • Individuals may not know who to contact if things go wrong • No one is prepared to take ultimate responsibility for fixing the problems and the individual is passed between the igovt logon service and the igovt IVS • There is no easy way to access a 24/7 support service; • The burden of security and other risk is placed on the individual through the 'Terms and Conditions'. • The assumption will be that the individual is at fault if something goes wrong.

11 FINDINGS ON PRIVACY RISKS AND RECOMMENDATIONS

11.1 PURPOSE OF COLLECTION AND IPP 1

11.1.1 COLLECTION FOR LAWFUL PURPOSE

IIS does not have any reason to believe that the collections proposed for the igovt IVS full service build are for anything but lawful purposes.

11.1.2 COLLECTION NECESSARY FOR PURPOSE

The collections proposed for the igovt IVS full service build appear to be consistent with the purpose of the igovt IVS, in particular, to ensure that the identity validation process is strong enough to create high confidence in assertions of identity information using the igovt ID.

11.1.2.1 SCANNING EOI DOCUMENTS

The key new collection resulting from the igovt IVS full service build is the scanning of identity and other documents that, in some cases, an applicant will be required to provide as evidence of their identity. Such documents could include:

- non-NZ passport;
- driver licence;
- non-NZ evidence of name change;
- non-NZ birth certificate;
- non-NZ marriage certificate;
- student identity card;
- building licence;
- professional registration.

These scanned documents will be stored in the Applications database of the igovt IVS and as a result, the igovt IVS will be storing agency specific individual identifiers, such as licence number, and document numbers from other organisations and agencies. IIS understands that the EOI and related documents are collected and stored in order to be able to resolve any disputes about the basis on which identity information has been asserted.

Although the igovt IVS is designed so that Person IDs and full name and document number used in the uniqueness process are deleted from the igovt IVS once the uniqueness process is completed, this will not be the case with individual agency identifiers or document numbers that are printed on scanned documents. This could undermine a key approach in the development of the igovt IVS (and the igovt logon service) which is to keep agency specific identifiers for individuals separate from the igovt IVS.

Another key risk is that by centralising such documents there could be temptation among law enforcement or other agencies to use the igovt IVS as a handy investigative resource. Access to scanned documents is not dealt with in the EIV Bill, unlike access to usage history, core identity information and photographs. IIS considers that to maintain User trust in the igovt IVS, DIA should take steps to ensure that access by law enforcement agencies for investigative purposes is well governanced and not an easy option. There also could be heightened security risks (discussed below in Section 11.5.3).

Recommendation 3 – Technology: Encryption of scanned documents and governance for access
IIS recommends that if scanned documents are to be stored in the igovt IVS they should be stored in encrypted form with very limited access to the encryption keys. There should be strong governance and accountability mechanism for deciding when access to the scanned EOI documents will be allowed. The EIV Bill should be amended to cover access to scanned documents as well as photographs.

Recommendation 4 – Technology: Reduce reliance on scanned documents
IIS recommends that DIA works with DoL and any other New Zealand agencies that are sources of EOI to develop the technology necessary to reduce the need for EOI and related documents to be stored in the igovt IVS. DIA should also determine when these documents will be no longer needed and a process for deleting them from the igovt IVS at that point.

11.1.2.2 Audit and logging
Information generated through data trails can be a means by which a system 'collects' unnecessary information.

A key risk with the igovt 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. With the addition of NZ Post at the photo capture stage and particularly with its integration role with the private sector, the potential to gain a wider picture of an individual's life increases significantly. There are, of course, many reasons why interactions may need to be logged and audited. However, it is important that DIA and NZ Post take a conscious and structured approach to deciding what will be logged and auditable. IIS notes that the EIV Bill significantly mitigates the privacy risk associated with accumulated logs through restricting access to usage history, including by law enforcement agencies who must obtain a warrant (see Clauses 21A and 21B of the EIV Bill).

Recommendation 5 – Business as usual and technology: Audit and logging
DIA (in conjunction with NZ Post where appropriate) should ensure there is a process for assessing which activities in the full igovt IVS build should be audited and logged. The process should ensure that activities are only logged if there is good reason consistent with the purposes of the igovt IVS full service build.

11.1.3 Steps to reduce unnecessary collection
IIS notes that the igovt IVS full service build has taken steps in a number of stages to ensure that information not essential for the function or activity of the igovt IVS or the agency participating in the application process is either not collected or deleted once its purpose of collection has been fulfilled. This includes adopting the approach that when source agencies check identity details against agency records, the information returned initially is only:

- Yes (match);
- No (no match).

11.2 Direct collection and IPP 2
On the information available to IIS so far, there does not appear to be anything proposed in the igovt IVS full build that would change this risk.

11.3 Notice and transparency and IPP 3

The igovt IVS full service build has added significantly to the complexity of the igovt IVS system and business processes. This includes through:

- the more complex EOI process including the process for checking source documents;
- use of NZ Post for the photo capture stage.

Service Users should be aware of those organisations participating in the igovt IVS full service build and the role they play. Service Users should also be aware that the details they provide will be checked with the relevant agency. These developments make real transparency more difficult to achieve, but not impossible. DIA and NZ Post will need to use a range of techniques for achieving this besides presenting a long document that no one reads. Strategies that can be used include:

- 'just-in-time' notice through information that appears when a mouse hovers over an area when information is to be entered (or placed down the side on a window by window basis);
- use of language that is easy to read and understand;
- 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.

Recommendation 6 – Business as usual: Informing Service Users
DIA should engage experts in plain language and online usability to ensure that Service Users are easily able to access and understand the important information about how igovt IVS and NZ Post (and any other participants) 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 privacy policies and corresponding changes to privacy notices as they occur over time.

11.4 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 igovt IVS full service build.

11.5 Storage and Security and IPP 5

11.5.1 Complex manual back office identity checking

IIS considers the igovt IVS full service build could create significant privacy and security risks including unintentional or accidental breaches, intentional but unauthorised breaches, and malicious breaches. igovt IVS back office personnel will have access to and be handling sensitive identity documents that will need to be carefully managed. Risks include that:

- identity documents that are printed from the igovt IVS are left on desks, removed from the office and lost, misplaced or misappropriated;

- phone conversations between igovt IVS back office staff and DoL or other source agencies exchange more information about applicants than is relevant to the application;
- personnel working nearby may overhear conversations about people they know;
- sensitive information and documents may be exchanged by unsecured email;
- sensitive data is sent to the wrong person by email or post;
- staff may use the information they handle to steal an identity, or to help someone else steal an identity;
- staff may be using identity information to earn money, for example, from private investigators;
- staff may disclose information to law enforcement agencies without proper authority;
- DIA staff working in other sections ask for information about people they know for the purposes of their particular line of non-igovt IVS related work;

Steps that DIA can take to handle these risks include (if not already in place):

- security screening of personnel working in the igovt IVS back office;
- a work area that is separate from other sections of DIA offices and has physical security access controls;
- limiting the printing of documents to cases of necessity and ensuring that people have printers nearby which are immediately cleared once printing is complete;
- keeping an audit trail of who has printed what documents;
- clean desk policies and lockable cabinets;
- policies around laptops and USB and other removable devices, and on removal of documents from the work place;
- policies and procedures for the correct handling of hard copy documents;
- training of staff on privacy and security that addresses the particular nature of their duties but also explains the underlying concepts so that staff can make good decisions in ad hoc situations;
- regular internal monitoring and audit of content of emails and also to check that policies and procedures are being implemented backed up by annual or biannual external audit.

IIS considers that DIA should get expert assistance in assessing the security risks associated with back office manual handling of identity information and document and implement policies and procedures to address them.

Recommendation 7 – Business as usual: Expert advice to assess and manage security risks in manual processing
IIS recommends that once the igovt IVS back office processes are more fully spelled out, DIA engage a security expert at both the development and implementation stage to assess the security risks of the processes and advise on how to minimise these risks.

Recommendation 8 – Accountability: Regular monitoring and audit of back office processes
IIS recommends that once policies and procedures for back office processing are in place, DIA regularly monitors, and conducts audits of, them to ensure that staff comply with them.

11.5.2 Access to the igovt IVS by external agencies and organisations

DIA has taken steps to addressed possible security risks that could arise from non DIA staff such as NZ Post staff and DoL staff having access to the igovt IVS system to perform their roles by:

- Business as usual: imposing strict security requirements in MOUs with government agencies and contracts with NZ Post;
- Law: having provisions in the EIV Bill, including offences for misuse and disclosure of information held in the igovt IVS;
- Technology: providing for roles based access which restricts access of DoL and NZ Post staff to the igovt IVS to only those applications that are relevant to their role in the application process and extensive logging of such access;
- Governance: - including provisions in the EIV Bill regarding who can have access to igovt IVS information and in what circumstances and provisions in agreements relating to audit and monitoring.

[redacted]
Withheld to prevent improper gain or advantage
[redacted]

In the igovt IVS full service build the applicant must bring their application number to the NZ Post Office and the photo capture operator will use the application number to retrieve the application. Also, the operator will enter, via a Consent screen, the fact that the applicant has consented to having their photograph taken. [redacted]

- [redacted]
Withheld to prevent improper gain or advantage
[redacted]
- [redacted]

[redacted]
Withheld to prevent improper gain or advantage
[redacted]

A risk could also be that it makes it easier for a NZ Post operator to access a person's records by guessing or using a person's application number. However, it is not clear what benefit this would achieve as every activity they conduct is logged and potentially audited.

DIA has considered these risks and has proposed some mechanisms to address them including:

- randomisation of the application number – to make it more difficult for an operator to guess a person's application number;
- an additional screen to manually capture the applicant's consent for photo capture;
- sending a text of the application number to the applicant on completion of the apply online stage – which links the application number to a particular phone number.

[redacted]
Withheld to prevent improper gain or advantage
[redacted]

11.5.3 Scanned documents

IIS considers that having a centralised system containing scanned EOI documents could create a valuable 'honey pot' of identity documents which those with malicious intent such as identity theft could devote considerable resources to get access to. As identified in Section 11.1.2 Necessary collection, the way to manage this risk is to encrypt the documents in the igovt IVS and, if possible, to reduce dependence on scanned documents over time, and then delete when no longer needed.

11.6 Access by Service User to information held in the igovt IVS and IPP 6

11.6.1 Access to captured photograph and scanned documents

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 EIV Bill (Clause 20A) 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).

Access to the captured photograph was not provided to Users in the initial implementation of the igovt IVS. The EIV Bill says that a Service User may access their captured photograph (Clause 20B).

IIS understands that DIA will make this possible via a manual business process where the individual would make an appointment with DIA to see the photo. The EIV Bill is silent on the question of access by Users to their scanned EOI documents that will be stored in the igovt IVS.

Service User access to their captured photograph and scanned EOI documents is a complex issue. The Privacy Act gives an individual a right of access where an agency holds personal information 'in a way that can be readily retrieved.' On the one hand, for control and transparency purposes, there is privacy benefit in making a person's captured photograph and scanned documents readily accessible, including, through their igovt ID web page. On the other hand, to make the photograph and scanned documents more secure and to discourage function creep there are very significant privacy advantages in the photograph and more importantly the scanned documents to be held in encrypted form in the igovt IVS. If it is a choice between one and the other, IIS' initial view is that there is greater privacy benefit for the individual in having particularly the scanned documents encrypted. This view takes into account the fact that the individual will have the original of the scanned document in their possession and request for access is likely to be rare.

Recommendation 9 – Technology: Balance between User access and protection through encryption
IIS recommends that scanned documents and photographs stored in the igovt IVS should be stored in an encrypted form.

11.6.2 Impact on access - involvement of NZ Post in photo capture process and integration

11.6.2.1 NZ Post photo capture

On the basis of the information that IIS has, NZ Post will hold very little information about a User arising out of the photo capture stage. It will only see the applicant's name and application number. The design provides that once photographs and scanned documents are uploaded they are deleted from NZ Post's system. There will be logs that track NZ Post Operator activities in relation to a particular application. If there is a dispute about what happened, the User should have a right of access to these if they hold any personal information about the User, but there does not seem to be any strong argument for this information being accessible through their igovt account.

11.7 Correction and IPP 7 and Accuracy IPP 8

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 EIV Bill specifically provides for a Service User to be able to access their igovt IVS record and usage history (Clause 4(e) principle, Clause 20A, Clause 21(1)(a)).

In the Initial Implementation DIA takes the approach that if a Service User finds that attribute information is wrong the Service User is referred back to Passports or Citizenship to have the information corrected there. This is because the igovt IVS obtains this information from the VISI which has passed on information obtained from Passports or Citizenship databases.

IIS considers that there is a significant risk that inaccurate identity information could be entered into the igovt IVS as a result of the many manual data entry processes involved in the igovt IVS full

service build. The main manual entry points will be the igovt IVS back office processes and DoL checking processes.

The risk of inaccuracy will be significantly reduced if DIA and DoL develop clear policies and procedures for the verification stage and train staff thoroughly in them.

Recommendation 10 – Business as usual: Policies, procedures and training for staff to avoid inaccuracies in data entered into the igovt IVS
IIS recommends that, to minimise inaccuracies in igovt IVS data, DIA and DoL develop detailed policies, procedures and training for igovt IVS back office staff and DoL staff involved in verifying information supplied by igovt ID applicants and other processes involved in the verification and image determination stages of an igovt ID application process.

Nonetheless IIS considers that there will remain a significant risk of inaccuracies, particularly until processes are properly bedded down. The EIV Bill assists in addressing this risk by including provisions (Clauses 26(1) and 26(2)) that enable an individual to apply to amend or correct their igovt ID in specified circumstances. The Bill also includes provisions that require DIA to take certain steps if it refuses to make such amendment or correction which, depending on the circumstances may include notifying the applicant, telling them the reasons for refusal, and telling an agency the information is disputed when the igovt IVS supplies the information to a participating agency (Clauses 26(5) to (5C)). DIA should make sure this process is easily accessible

Recommendation 11 – Safety-net: Helping Service Users correct inaccuracies
IIS recommends that DIA provides easily accessible help for individuals seeking to correct their igovt ID using the processes provided for in the EIV Bill. DIA should monitor the incidence of inaccuracy of information held in the igovt IVS in order to identify and address any inaccuracy problems with its or DoL's administrative processes relating to the application and issuance of igovt IDs.

11.8 Retention of igovt IVS information and IPP 9

Given the identified privacy risks associated with storing scanned EOI documents in the igovt IVS a key question is how long such documents should be kept, and whether it will be possible to delete at least some of them when, for example, the new DoL records system is in operation.

IIS notes that although the EIV Bill will require DIA to make regulations specifying how long it is allowed to keep igovt ID information (including status information and FITs), usage history records and photographs, it does not address the issue of retention of scanned EOI documents.

Nonetheless DIA should consider the question and make a schedule for deletion of scanned documents at the same time as it prepares the regulations. IIS considers that the igovt IVS system should be designed to enable the deletion of scanned documents if, for example, more automated checking processes are in place in DoL or other source record agency, which give a User the option of undergoing an automated verification process.

IIS recognises that some record checking will always have to be by manual process, and that it is likely that scanned copies of these will need to be retained in the igovt IVS at least for a significant period.

Recommendation 12 – Business as usual and technology: Deletion of scanned documents when automated processes available

IIS recommends that DIA develops a schedule for deletion of scanned EOI documents. In addition igovt IVS full service should be designed in a way to make it possible to delete scanned documents in the future should automated means of checking EOI documents become available. This could include offering Service Users the option of undergoing a process that will remove the need to store their scanned EOI documents and enable them to be deleted from the igovt IVS.

11.9 Reports

The igovt IVS full service build will enable a wide range of reports to be generated about igovt IVS activity. It will include the ability to generate reports about the number of transactions of a specific igovt ID that have occurred in a particular month (PF5). It also has inbuilt ad hoc reporting capability to meet future needs (PF10 Managing igovt IDs).

IIS considers that there could be a risk that reporting could be used to extract information about the behaviour of a particular igovt ID holder which could be useful for purposes unrelated to the igovt IVS service. This could potentially proceed with little scrutiny if the reporting system has inbuilt flexibility to accommodate future change.

Recommendation 13 – Business as usual: Reporting

IIS recommends that there should be a process for assessing what reports are and are not necessary for ensuring the proper operation of the igovt IVS and flowing from this, rules about what reports relating to the operation of the igovt IVS are, and are not, allowed and in what circumstances. DIA should establish a change and governance procedure to ensure that changes to the types of reports conducted are assessed to ensure they are only generated for purposes consistent with the igovt IVS.

11.10 Unique identifiers and IPP 12

There are two changes to the way identifiers are handled in relation to the igovt IVS full service build. One is the introduction of the application number to the igovt ID apply process. The other is a change to the way that Person IDs are linked to FIDs to ensure uniqueness.

IIS has not identified any issues relating to unique identifiers that might create concerns in relation to IPP 12. However, a key issue with identifiers can be that they are used to link people and their activities across agencies.

11.10.1 Application number

IIS considered the question of whether the introduction of an application number might create a risk that it could be used to link the activities or information about the igovt ID holder across agencies. IIS considers that it is unlikely that the application number would be used for this purpose. It is stored in the igovt IVS application database but not used in any other context once the application is complete.

11.10.2 Process for ensuring uniqueness

Due to the additional EOI sources (immigration and birth) that an applicant can now use to apply for an igovt ID with, additional checks must be conducted on all igovt ID applications to ensure that the

person has not previously been issued with an igovt ID and cannot be issued with another one at any stage based on any of the other available authoritative sources of EOI. This process for establishing 'uniqueness' may require a Person ID and/or full name and document number to be manually entered into the igovt applications system of the igovt IVS to invoke the automated uniqueness check performed by the VISI against the Federated ID Service and to enable the VISI to return a FID to the igovt IVS.

This undermines a key principle underpinning the igovt IVS and the reason for establishing the VISI which is to keep agency person IDs separate from the igovt IVS.

However, DIA has sought to address this issue by ensuring that the Person ID and full name and document numbers are deleted from the igovt IVS system once the VISI has linked a PID to a FID and sent the FID to the igovt IVS to be linked to the igovt ID.

11.11 Choice and control

11.11.1 Notification of change of status

IIS considers that there is the possibility for loss of control of information about Service Users in the case where changes are made to a person's igovt ID status.

The EIV Bill (Clause 20(2)(a)) requires the chief executive to notify a relevant participating agency if an igovt ID has been revoked. It also authorises the chief executive to notify a participating agency of other changes if, in the opinion of the chief executive it is in the participating agency's interest to receive that information. This is a broad discretion which IIS considers should only be exercised when it is necessary for the purpose of maintaining the integrity of the igovt IVS. It should not be used where it might assist the agency to begin a general investigation of the affairs of an individual, for example.

Recommendation 14 – Business as usual: Assess in detail notification of igovt ID status
IIS recommends that DIA develop a guideline which outlines the basis on which it will exercise its discretion under Clause 20(2) of the EIV Bill to provide information about a change in status of an igovt ID to an agency participating in the igovt IVS. The guideline should ensure that DIA only exercises this discretion when it is necessary for a purpose that is directly related to the purposes of the igovt IVS. DIA should consult with the Privacy Commissioner in developing the guideline.

11.11.2 Loss of control over time due to increased reliance on the igovt ID

An important underpinning principle for the igovt ID is that using or gaining one is to be entirely voluntary (Section 4 (1)(a). It is also important to recognise however that overtime the protecting power of this principle fades as government and private sector increasingly rely on online means of transacting with individuals, and the igovt ID to facilitate such transactions. In these circumstances, the use of the igovt ID will inevitably become the default approach. Individuals will find it increasingly difficult to conduct their lives unless they have and use an igovt ID.

This is not a matter to make a recommendation about at this stage. However, it underlines the importance of not placing too heavy reliance on choice for privacy protection and gaining trust. It requires there to be a whole range of other mechanisms to protect individual privacy and to gain trust besides choice.

11.12 UNFAIR OR INAPPROPRIATE ALLOCATION OF RISK

As identified in the previous PIA on the igovt IVS 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.

IIS considers that, in particular, the question of ensuring there is a smooth, coordinated, accessible and responsive inquiries and complaints mechanism remains an issue.

IIS heard anecdotal evidence of several cases where people that experienced difficulty with the initial implementation of the igovt IVS had trouble gaining a solution to their problem. It appears that they were passed between BDM and the Customer help line with no one taking responsibility for mediating between the two agencies to find a solution.

These may have been low in numbers, and IIS may not have heard the full story. DIA may have changed its processes since then. However, it does raise issues about the extent to which the current inquiries and complaints handling mechanisms are adequate to cope with the additional inquiries and complexities associated with the igovt IVS full service build including the manual processes, the inclusion of another, and a private sector, partner, and the complexities of handling the kind of integration process proposed.

The fundamental principle here is that if the igovt IVS or integration layer appears to the User to be one service, then inquiries and complaints MUST be handled as if it is one service, one-stop-shop. There must be no 'buck passing' and there must be no circumstance in which the individual is left to decide who to approach next when a problem is not resolved.

Recommendation 15 – Safety-net: Review of inquiries and complaints handling processes
IIS recommends that DIA reviews its inquiries and complaints handling processes to assess whether they are sufficiently coordinated and responsive to handle the increase in number and complexity of inquiries and complaints that will occur with the igovt IVS full service build and the addition of NZ Post as a partner. DIA should ensure that it discusses in detail the processes to be followed by NZ

Post to ensure that the increase in integration at the process and the technology level is accompanied by a smooth, one-stop-shop integration at the human and customer service level. DIA should ensure it collects data about complaints processes (internally and from Users) and regularly reviews it for continuous improvement in its processes.