PRIVACY IMPACT ASSESSMENT

ENHANCED PROVISIONING FOR AUS.GOV.AU

For: Department of Finance and Deregulation

29 SEPTEMBER 2011

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

1.1 INTRODUCTION

The Department of Finance and Deregulation (Finance) has engaged Information Integrity Solutions (IIS) to conduct a Privacy Impact Assessment (PIA) of enhancements to the australia.gov.au account provisioning process.

The project will enable agency customers to link their australia.gov.au account to agency records in a simplified manner from australia.gov.au. This new process will allow agencies to decommission their existing credential provisioning systems.

Finance asked IIS, through the PIA, to identify:

- all specific breaches of the Government's legal obligations to its customers that would be created by the solution design (and recommendations for resolution of these); and
- any best practice ideas that could improve the privacy protection behaviours of the solution.

This project is a collaborative effort with other agencies: DHS in particular. As a result IIS has provided a high level overview of the end-to-end solution in its PIA.

However, IIS has received very limited information about the DHS part of the new provisioning system. It is therefore not in a position to make any definitive finding on the privacy impacts arising from the way DHS has developed its part of the system. IIS understands that DHS is conducting its own PIA.

The main focus of this PIA is therefore on those components managed by Finance.

In undertaking the PIA IIS:

- consulted with Finance and finalised the work plan;
- gathered information which included:
    - a number of documents; and
    - meetings with key Finance personnel;
- prepared a first draft of the report;
- received feedback from Finance;
- received further detailed documentation;
- had further discussions with Finance;
- prepared the final report.

1.2 FINDINGS

The key privacy concern with an initiative which involves a centralisation of access to government services is that it could lead to linking of information about a person across agencies and a consequent whole of government picture of the life of an individual. It could lead to information provided for one purpose being used for other new purposes that the individuals do not want or expect.

On the flip side, there is a significant risk that, while information might be received in a streamlined centralised process, when things go wrong, the response is far from streamlined or whole of government.

IIS initially assessed australia.gov.au, the GSE and the GSE hub in 2007 and found that they were designed both from a technological and business process point of view to minimise these risks. The new account provisioning process builds on this infrastructure and IIS considers that overall, the additional functionality is achieved without significantly adding new privacy risks. IIS considers that there might be potential risks arising from the DHS part of the new provisioning system but, privacy assessment of this was out of scope for this PIA and in any case, IIS did not have sufficient information to make any finding on this.

The technology for achieving federated authentication is rapidly evolving in a way that continues to reduce the risks of linkage that they can give rise to and IIS makes a recommendation about this.

The new provisioning process is only one step in a number of others to follow which are designed to simplify individuals' interactions with government. As with its previous assessment, IIS considers that, as the GSE capability is expanded, properly managing the change to ensure that it has community trust and acceptance will be the most important issue. Whole of government initiatives require whole of government governance. To this end, IIS makes recommendations about good process and governance.

1.3 LIST OF RECOMMENDATIONS

Recommendation 1 – Technology: Monitor and adopt best practice federated authentication technology

IIS recommends that Finance should monitor technology developments in the area of federated authentication that could further reduce the risks of linkage that arise from the use of the GSE Authentication Hub. Where practical and appropriate it should seek to adopt best practice technology as the Hub becomes an increasingly central part in whole-of-government online authentication.

Recommendation 2 – Business as usual: A documented process for identifying and managing major change having privacy implications

IIS recommends that Finance documents a process for identifying and managing privacy in relation to proposed major policy and technology changes to the GSE. The document should formalise the approach that where changes to the GSE are identified as having significant privacy implications the process should include a privacy impact assessment and a means for public scrutiny, including community consultation and potentially parliamentary scrutiny.

Recommendation 3 – Business-as-usual: Information about where to find out reasons for unsuccessful account provisioning process

IIS recommends that where an individual is told during the account provisioning process that their question and answer session has been terminated and the account linking process unsuccessful, the GSE should ensure that the individual is told where he or she can get more information about the reason why the account provisioning process was unsuccessful. The process for getting more information should be readily accessible and user friendly.

Recommendation 4 – Governance: Independent policy making body for GSE including Hub

IIS recommends that Finance take steps to implement a governance structure for the GSE including the GSE Authentication Hub that is independent from any one particular Australian Government agency. It should include:

- A CEO that is not part of a line agency structure of responsibility;
- A board with power to determine policy and make important operational decisions. The Board should have a mix of representatives from relevant government participating agencies and include a significant component of consumer / citizen representatives and a recognised privacy expert.

2 INTRODUCTION

The Department of Finance and Deregulation (Finance) has engaged Information Integrity Solutions (IIS) to conduct a Privacy Impact Assessment (PIA) of enhancements to the australia.gov.au account provisioning process.

The project will enable agency customers to link their australia.gov.au account to agency records in a simplified manner from australia.gov.au. This new process will allow agencies to decommission their existing credential provisioning systems.

2.1 PURPOSE AND SCOPE OF THE PIA

The PIA is of the proposed technical solution for the enhancement of the provisioning process for australia.gov.au. This is the second draft of the report IIS has prepared as part of this process. The solution was still in development when IIS prepared the first draft PIA which was an initial assessment of the proposed solution.

Further detailed design has now been completed, and this final report takes into account feedback IIS received from Finance about the first draft of the PIA as well as any new issues IIS has identified from the more detailed documentation provided.

Finance has asked IIS, through the PIA, to identify:

- all specific breaches of the Government's legal obligations to its customers that would be created by the solution design (and recommendations for resolution of these); and
- any best practice ideas that could improve the privacy protection behaviours of the solution.

This project is a collaborative effort with other agencies: DHS in particular. As a result IIS has provided a high level overview of the end-to-end solution in its PIA.

IIS has received very limited information about the DHS part of the new provisioning system. It is therefore not in a position to make any definitive finding on the privacy impacts arising from the way DHS has developed its part of the system. IIS understands that DHS is conducting its own PIA.

The main focus of this PIA is therefore on those components managed by Finance.

This final PIA builds on our review of initial documentation and discussion with Finance, and subsequent new solution design documentation provided by Finance.

2.2 METHODOLOGY

In undertaking the first draft of the PIA IIS took the following steps:

- consulted with Finance and finalised the work plan;
- gathered information which included:
    - reading the following documents:
        - GSE Authentication and australia.gov.au Account Roadmap v1 0

        - GSE Online Provisioning Detailed Business Requirements v0.10 8/07/2011
        - Government Services Environment DHS Online Account Provisioning Solution Architecture v 07;
        - Interim Service Level Agreement Centrelink and the Department of Finance and Deregulation for IT Support and Maintenance for the Whole of Government Authentication Hub Single Sign on Service;
        - Memorandum of Understanding between Department of Finance and Deregulation (Finance) and Department of Human Services (DHS) August 2011 V0.6;
        - Audit and Logging Design for the Australian Government Online Service Point AGOSP Solution, Final Version 1.2 2008;
        - Customer Support Processes for the Government Services Environment (GSE) v 1.0 1/6/2011; and
    - a phone call and meeting with Finance personnel to discuss and clarify details of the technical solution;
- analysed the technical solutions against the Information Privacy Principles (IPPs) in the Privacy Act 1988 (Cth) and other privacy risks and best practice issues that could arise that go beyond compliance with the law;
- prepared a draft report which Finance gave initial comments on.

In preparing this second draft of the PIA IIS:

- read the feedback it received from Finance;
- read the further documentation Finance provided:
    - GSE Online Provisioning Detailed Business Requirements, AGIMO, 02/09/2011, Version 1.0
    - DHS SDR Connected Authentication Release 2: GST Online Provisioning, Test Strategy, AGIMO, 16 August 2011, V 0.20
    - UCD Test Plan
    - User Interface Design for the DHS SDR Connected Authentication Release 2: GSE Online Provisioning, 29 August 2011, v 0.3
    - User Interface Design for the PORO project, 22 August 2011 v 0.2
    - Government Services Environment (GSE) DHS Online Account Provisioning High Level Design 01/09/2011, v 1.0
- had some further discussions with Finance;

- finalised the second version of the report which includes refined detail about the project, initial and further risks identified and recommendations in relation to privacy risks and best practice privacy issues identified.

In developing its recommendations IIS draws on its 'layered defence' approach. This applies a number of possible 'tools' to arrive at practical solutions that fit the particular circumstances. These tools include:

- 'business as usual' good policy and practice, including education, process and culture change regarding the way things are done by staff, and the actions that users need to take to protect themselves;
- additional law where risks are particularly high (eg specific use and disclosure limitations, criminal penalties, special measures to ensure review before critical changes are made;
- technology, including design limits on information collected, what can be connected and who can see what;
- governance, including transparency and accountability;
- safety-net mechanisms including an easily accessible complaint mechanism for affected citizens when failure or mistakes occur.

3 CONTEXT FOR NEW PROVISIONING PROCESS

On 2 May 2007 the (then) Special Minister of State, Gary Nairn, announced a $42.4 million budget initiative that would enhance the australia.gov.au website to provide a personalised entry point to government for individuals. This was called the Australian Government Online Service Point (AGOSP) project.

AGOSP project sought to be a one-stop-shop for users to access information and services provided by the Australian Government. It aimed to give citizens a primary point of access to online services and information provided by any agency of the Australian Government.

From 2008 individuals could establish an AGSOP account at the australia.gov.au website. An individual could link their AGOSP account to another online agency account. Once the link was made they could log on to their AGOSP account and then access the agency's online account without having to go through another log on process using their agency credentials (single sign-on).

On 16 December 2009 the Minister for Human Services announced that he was seeking to simplify the means by which people could access human services, including through having a single phone number, a single website and a single credential. The Department of Human Services (DHS) sought to achieve this vision through its Connected Authentication Project.

In April 2011 DHS entered into a collaborative project with AGIMO to use the australia.gov.au individual account facility as a key means of meeting its Connected Authentication Project objectives. This collaboration also advances AGIMO's objective of furthering the use of the Government Services Environment (GSE, previously called AGOSP) and advancing its australia.gov.au Authentication Roadmap. This Roadmap sets out three phases of proposed development to enable

increased use of the australia.gov.au account by Agencies for online authentication and to assist in the delivery of new services for individuals related to common information or changes in circumstance. The developments will also allow the reuse of information previously supplied to the Government by individuals.

The collaboration project involves establishing additional australia.gov.au capabilities to assist with offering a common, Whole of Government online registration pattern. australia.gov.au already has the underlying applications; however some development is required to implement the required processes and capabilities.

There are three main goals of the collaborative project. These are:

1. to allow an Authenticated User to link their australia.gov.au account to their Agency Security Account's (ASA) by answering a number of questions provided to australia.gov.au from a program within the Department of Human Services (DHS). This is known as the Proof of Record Ownership (PORO) process.

2. to allow an Authenticated User to link their australia.gov.au account to their Agency Security Accounts (ASA) by providing an activation code and an Agency Reference number (ARN). This is known as the Activation Code Process.

3. to implement goals 1 & 2 in such a way that it can be extended for use by other agencies.

4 DESCRIPTION OF THE NEW PROVISIONING PROCESS

4.1 ENTITIES IN THE NEW PROVISIONING PROCESS

The following are entities involved in the new provisioning process:

- the individual

- the GSE – This is a technology platform that enables cross-agency service delivery by the Australian Government. The GSE uses the australia.gov.au website as its public front-end and includes an Authentication Hub service (GSE Hub).

- the GSE Hub – this enables a user to establish credentials for an australia.gov.au account, link their australia.gov.au account to an existing agency online account (single sign-on) and enable the user to manage their australia.gov.au account credentials (eg change password, replace secret questions and answers.

- DHS – DHS is the service user for the new account provisioning service provided by the GSE. It also operates the GSE Hub as a service provider on behalf of the Department of Finance. The Government has nominated DHS as the lead agency for whole-of-government people-to-government (P2G) authentication.

- master programs – the following DHS programs are called master programs for the purposes of this project.

    - Centrelink;

- Medicare;
- Child Support Agency.

The new provisioning process will enable an individual to use their australia.gov.au account and credential (username and password) to establish and use an online account with any or all of three DHS master programs with whom they already have a relationship.

australia.gov.au currently enables an individual to use their australia.gov.au credential to access an online account with one of these master programs. However, an individual is not able to do this if they have not already separately proved to the agency that they 'own the record' they are seeking access to and have an agency specific credential they can use in the first instance to link to their australia.gov.au account.

The new provisioning process will enable an individual to prove they own the record and establish an online account with the relevant master program in one interaction mediated by australia.gov.au as a front end to the GSE without having to first establish proof of record ownership with the relevant master program and being issued with a separate credential.

4.2 AUS.GOV.AU ACCOUNT

If the individual does not already have an australia.gov.au account, they will need to establish one before they can use the new account provisioning process. This is an existing functionality and will not change.

4.3 PROOF OF RECORD OWNERSHIP PROCESS

In the new provisioning process individuals will be able to prove ownership of a master program record through a question and answer process mediated through the individual's australia.gov.au account and the GSE. DHS will provide the GSE with a list of pre-set possible questions that individuals might be asked to establish proof of record ownership (PORO). DHS will use an algorithm to determine the actual questions to be asked in relation to the particular individual seeking PORO.

Once an individual has established and logged on to their australia.gov.au account they will be asked whether or not they have an activation code for the particular agency they are seeking to link to. If they have an activation code, they will be able to enter the code, their Agency Reference Number (ARN) and possibly some other yet to be determined questions and PORO will be established. The question and answer session will be complete.

An ARN is the number assigned to an individual by an agency for the purposes of the operations of the agency. It uniquely identifies that individual in relation to the agency. In the case of Medicare online, for example, it is the individual's Medicare number.

If the individual does not have a code, the individual will be asked an initial set of questions. DHS will require the GSE to ask each individual:

- given name (first name);
- family name (last name, surname);

- date of birth;
- gender;
- address;
- (email address - in future functionality, not in first release).

Then based on the initial information the individual has provided, the DHS algorithm will determine what further more targeted questions the GSE is to ask the individual. IIS understands that the number and nature of the further questions is determined on the basis of the answers to the questions and the risk profile of the individual.

The targeted questions are likely to be specific to the individual's interactions with the specified master program such as past benefit payments, or previous contact details.

Individuals with a low risk profile are likely to receive fewer questions. On the other hand, individuals who, for example have had a history of providing wrong addresses or giving false names, might require more questions, or be precluded from having an online account at all.

The GSE only acts on the instructions from the DHS system and plays no role in determining the type of questions it asks. The GSE has some role in determining the format of the questions.

The GSE also has no role in determining the answers the individual provides apart from ensuring some aspects of format and limited validations. It will not, for example, check an answer against any information the individual has provided for their australia.gov.au profile.

If the question and answer process results in the individual being unable to establish PORO or is rejected as ineligible to have an online account the GSE terminates the process and tells the individual that they have not been successful in establishing an online account with the relevant master program.

An individual can select more than one master program to link to. In this case, the individual will be taken in sequence through the questions that need to be answered for each master program they have selected to link to.

This is a new service provided by the GSE.

The technology being developed to enable this process is intended to provide the platform in the future for online form filling and information provision to other agencies who may wish to use it.

4.4 PREFILLING AND UPDATING

In future releases, the new provisioning process will, in the course of the question and answer process, give the individual the option of using an answer to a DHS question to fill in their australia.gov.au account profile (to the extent the fields are present in the profile), or to update information in their australia.gov.au account profile. However, this functionality is outside the scope of this release of the new provisioning process.

In this release the individual may be given the option to prefill questions asked in the DHS question and answer process with information from their australia.gov.au profile. However, it is a low level requirement and may not be implemented. If when it is implemented, the individual will be given the chance to overwrite the prefilled information before it is sent to DHS.

The individual will be able to choose whether or not they want to use these prefill or update capacities.

Data fields that individual can choose to fill in in their australia.gov.au account are:

- name;
- title;
- date of birth;
- address;
- email address;
- telephone number;
- country code;
- preferences;
- interests.

This dialogue and prefilling capability will also provide the basis for a process in the future for tell once and communicate many times capability. However, this extended capability is not part of this enhanced account provisioning project.

4.5 THE LINKING PROCESS

Once the DHS system is satisfied that the individual 'owns the record' it tells the GSE that this is the case. The GSE then asks the GSE Hub to create the necessary link (MBUN) for the relevant master program.

The GSE Hub uses the individual's GSE MBUN to find the individual's Hub record. Having found the record, the GSE creates a new MBUN which it sends to DHS to associate the individual with their master program online record.

As will all MBUNS issued by the GSE Hub, this MBUN will only be used for interactions between the individual and the particular master program record. It will not be used or shared with any other agency or between master programs. Design constraints which prevent sharing have been incorporated into the architecture.

When the relevant master program has successfully associated the MBUN with the individual's master program online account it sends a message to the GSE Hub confirming this.

The GSE confirms to the individual and DHS that the link has been made.

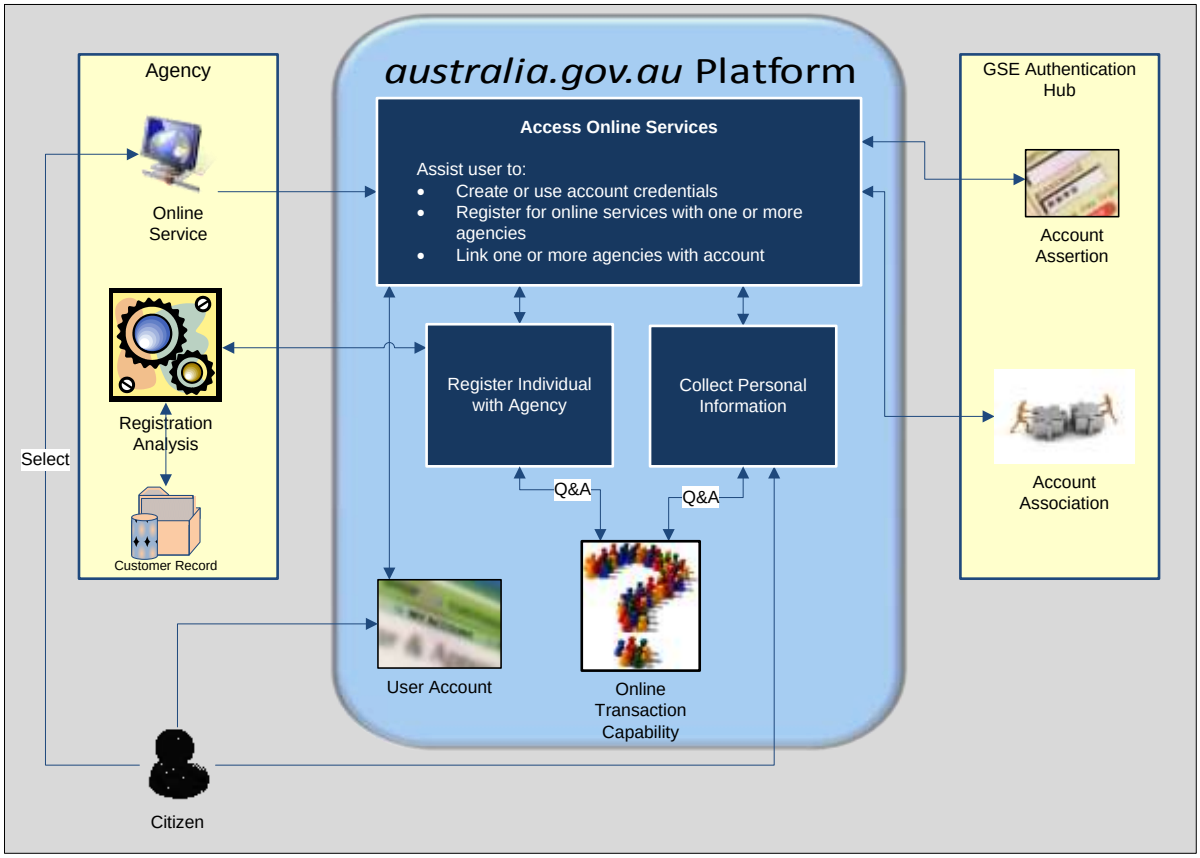
4.6 INTERACTION ID

A key change from the current linking process to the new account provisioning process is that a interaction ID is attached to each step in the end-to-end provisioning process, including the step in which the GSE Hub sends the MBUN to DHS and the master program.

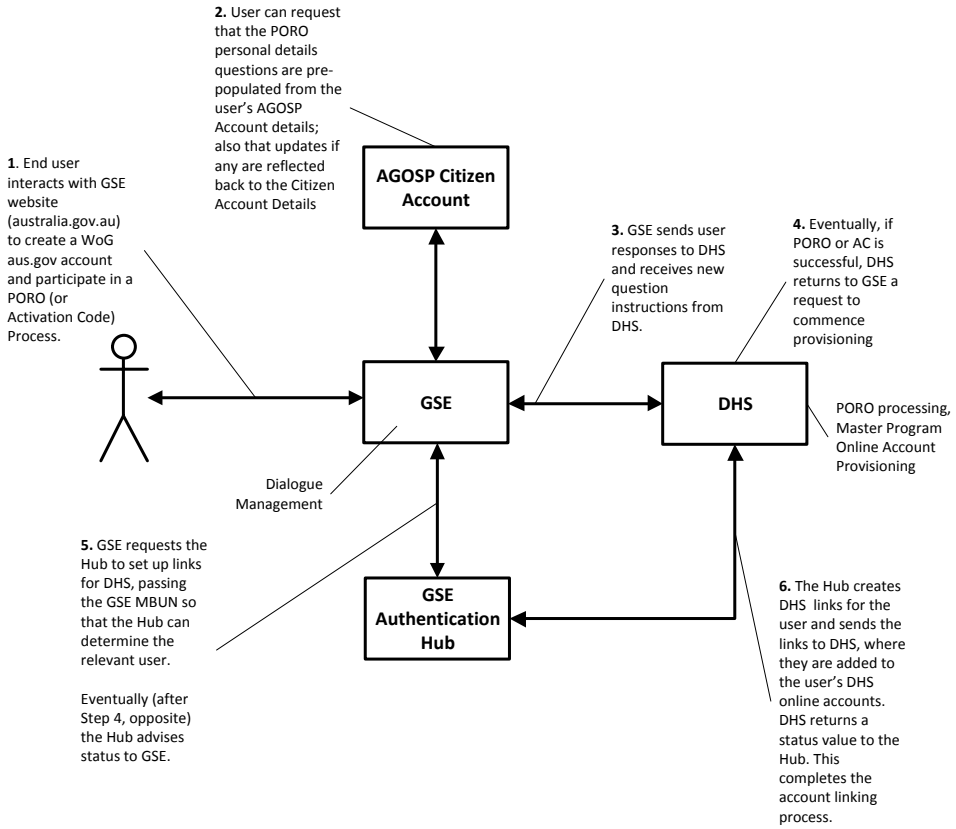
This enables the master program to associate the MBUN it receives from the GSE Hub with the particular PORO session the GSE has mediated between the individual and DHS and the master program.

5 DIAGRAMS

5.1 SYSTEM OVERVIEW AND CONTEXT



5.2 GSE ONLINE PROVISIONING



6 IPPS AND GSE ONLINE PROVISIONING PROCESS

The following section analyses the enhanced provisioning process against the Information Privacy Principles in the *Privacy Act 1988* (Cth).

6.1 IPP 1 MANNER AND PURPOSE OF COLLECTION OF PERSONAL INFORMATION

It is a key privacy principle that organisations should limit the collection of personal information to that necessary for a function, activity or purpose. For agencies this principle is embodied in IPP 1, which says that agencies can only collect personal information:

- For a lawful purpose that is directly related to their functions and activities; and
- If collecting the information is necessary for or directly related to that purpose.

Agencies also must not collect personal information unlawfully or unfairly.[1]

6.1.1 FINDING

There does not appear at this point in the development of the new provisioning process any clear evidence that it might not comply with IPP 1.

There does not appear to be anything intrinsically unlawful about the collection of information by the GSE, the GSE Authentication Hub or DHS and its master programs. Use of the new provisioning process is voluntary and users can choose whether or not to provide information necessary to

[1] The full text of the IPPs is available online at http://www.privacy.gov.au/publications/ipps.html.

establish PORO and an online account. Pre-population and updating options are also voluntary. Therefore there does not appear to be anything immediately obvious as being unlawful or unfair about the means of collecting information for the enhanced provisioning process.

The design of the provisioning process appears to have been consciously developed with limitation of the collection/storage of information by each of the entities involved to that which is necessary for the purposes of its functions in mind.

The GSE does not keep a record of the questions asked or the responses. It stores the interaction ID in an audit log with date and time stamp.

Also, DHS does not keep a record of the specific questions and answers. The DHS system stores Interaction IDs in an audit log with date and time stamp. DHS does not collect the individual's GSE MBUN in the course of the question and answer mediation session. GSE only shares this with the Hub.

As identified in first PIA that IIS conducted on AGOSP, the GSE Authentication Hub is specifically designed so that it does not need to collect personal information. It only collects user name and credentials such as password which does not need to be, and mostly will not be, personal information in the hands of the GSE Hub. It generates an MBUN which by itself is not personal information.

The following table shows what key information is collected in each of the entities involved in the provisioning.

Information collected/stored by the participants in the new account provisioning process

GSE	GSE Hub	DHS

Stored
• List of questions it is possible to ask
• Individual's account profile information (if completed)
  • name
  • title
  • date of birth
  • address
  • email address
  • telephone number
  • country code
  • preferences
  • interests.
	Stored
	• user name and password
	• The MBUNs that the credential has associated with it;
	• The agencies that the credential has linked to it;
	• The NeAF rating of the credential.
		Stored
		• agency reference number (ARN) and other information about the individual stored already for operational purposes
		• master program MBUN attached to the identifier
		• risk profile of the individual

Memory While Q & A in train as java object • Individual's GSE MBUN (within the session) • SAML header saying MBUN is OK (within session) • questions asked (until move to next page) • responses to questions (until move until next page) • ARN (within the session)	Memory (while passing through Hub) • Interaction ID	Memory • Interaction ID
Audit logs of • every time a profile is updated (existing functionality) • every time there is a dialogue ie Q and A session (new functionality) • link requests (new functionality)	Audit logs • Interaction ID • every time a person is logged in (existing) • other existing logs	Audit logs • Interaction ID with date and timestamp • requests to commence provisioning • status value of link sent

• termination requests by the agency and reasons (new functionality) • account associations (new functionality) • Interaction ID (new functionality) Tibco All requests and responses are logged in Tibco database for 7 days for support, troubleshooting, problem investigation purposes (existing functionality)		

6.2 IPP 2 AWARENESS AND TRANSPARENCY

It is a key privacy principle that individuals should understand why information about them is being collected and what will happen to it once it is collected. Where individuals have a choice about whether to provide the information this understanding enables individuals to make a decision about whether or not to give their information. It is an important element of giving individuals some control over their personal information.

For agencies, this principle is embodied in IPP 2 which says that when an agency collects personal information directly from the person who that information is about, it has to take whatever steps are reasonable to make sure the person is aware of these details:

- Why the agency is collecting the information
- The agency's legal authority (if any) to collect the information and
- To whom the agency usually gives that kind of information.

6.2.1 FINDING

Agencies normally implement this principle through a privacy notice that is given at the point of collection. In the case of a web site, agencies usually provide the notice on the home page of the web site. It is not possible yet to assess the provisioning process against this IPP yet as decisions about this are still in the early stages.

In the case of the new provisioning process achieving transparency will be more difficult than in the current account linking process because in many cases, rather than being redirected to the agency website to initiate the link, the individual will only be directly interacting with australia.gov.au for the provisioning process. As a result the information to be supplied through australia.gov.au relating to the provisioning process in compliance with IPP 2 will need to cover DHS and the relevant master program/s as well as the GSE and the Hub. The necessary consents will also need to be gained at this point including to all the terms and conditions.

6.2.2 GUIDANCE

IIS provides the following guidance about how to manage this requirement in the most user friendly way possible.

- one privacy notice on the australia.gov.au homepage web site will not be sufficient to give users the level of control they should have over their personal information.
- information such as why information is being collected, who is collecting the information and what happens to the information should be provided at the point where information is to be entered or where the individual must make a key decision rather than in one big piece of text which is accessed by a link at the bottom of the page called 'privacy'.
- consents should not be bundled into one inseparable list and should be given at the point each decision has to be made.
- Finance has already shown leadership by adopting agreed world best practice by implementing Multi-layered Notices for *australia.gov.au*. Using this approach for the enhanced provisioning process in addition to the above approaches will help to build trust in the service. However, IIS recognises that providing multi-layered notices where there are a number of agencies involved is more complex.

6.3 IPP 3 RELEVANCE, COMPLETENESS, CURRENCY AND NON-INTRUSIVENESS

IPP 3 requires that where an agency must collect personal information for a purpose, it should be relevant, up-to-date taking into account that purpose, and collected in a way that does not intrude unreasonably on the personal affairs of the individual concerned.

6.3.1 FINDING

At this stage, IIS does not have any information that would suggest that the new provisioning process would be at risk of non-compliance with this principle. However, Finance will need to establish business rules to ensure ongoing compliance with this principle.

6.4 IPP 4 STORAGE AND SECURITY OF PERSONAL INFORMATION

IPP 4 requires an agency to take reasonable steps to protect information from unauthorised access, use, modification or disclosure or other misuse, including when it is in the hands of an outsourced service provider.

Security risks can arise through inadvertent, intentional or unauthorised activities of internal staff and also through malicious activities from outsiders, such as hackers.

6.4.1 FINDING

On the information so far, it appears that the new provisioning service will have significant security benefits over the current account linking process. The provisioning communication process will occur through a web service back channel, system to system, rather than via the current approach using URLs which are redirected. This reduces the risk of a URL being diverted to another unauthorised system. As a result messages travelling between the GSE and DHS are not encrypted. However, the agency ID used to establish that each is communicating with the right person is encrypted.

IIS finds that there does not appear to be any easy way for GSE administrators to be able to view questions and answers travelling to and from DHS.

Questions and answers and the persons' ARN, whilst the data object is created and being prepared for transmission, will be in memory managed by the Tibco server. IIS was concerned that this might create a privacy risk, however IIS understands that it is difficult to view the memory and only when there is a failure will a memory dump file be created. To view the data contained in a memory dump file requires dedicated software and access to the system files associated with Tibco.

IIS was told that while there is a facility for a Tibco administrator to view the data if the Tibco server is started up in DEBUG mode. This action is extremely unlikely to occur as it would require the prior approval of AGIMO Change Advisory Control Board and Director of Service Management. Starting the server in DEBUG mode would place enormous overheads on disks space and performance. Starting the server in DEBUG mode would be logged in the Tibco auditable security event report.

Having discussed this issue with Finance, IIS has been advised that the Assistant Director of Service Management has added TIBCO auditable security event report to his list of saved reports that he will review on a regular basis.

Tibco also logs in its database all GSE service requests and responses for 7 days for support, troubleshooting and problem investigation purposes. The log is viewable through the Tibco administration console. This is existing functionality. There is a possible risk that an administrator may seek to view this information for in appropriate purposes. There are security measures in place to restrict access to the Tibco console to Business as Usual Support staff only. Rules restrict viewing the log on a needs only basis. Access to the Tibco console is audited by the administrator and logged for reporting.

IIS understands that Centrelink as agents of Finance, conducts an annual DSD Infosec Registered Assessor Program assessment (IRAP) of the environment which includes ensuring that processes are in place to protect sensitive data, such as audit trails and review of these, intrusion detection systems, review of system architecture for security holes and review of administrator access rights.

Taking into account these measures, including the strict monitoring of access and the change control process, IIS considers that there is a low privacy risk relating to the inappropriate use of or access to question and answer information and the ARN.

6.5 IPP 5 Awareness of personal information held by an agency

IPP 5 requires an agency to enable a person to find out if the agency holds personal information about them and, if so, the nature of the information held, the main purposes for which it is used and the steps necessary to gain access to the record. It must also publish annually in the Privacy Digest a range of information the Agency holds.

6.5.1 Finding

Our initial assessment is that apart from information held in logs and for a short time in GSE memory, the new provisioning process will not result in any of the participating entities storing more information about an individual than under the current arrangement. So the current arrangement for achieving this will still apply.

In the case of the GSE, an individual can see through their australia.gov.au account the information stored in their profile, changes made to their profile and information about the agencies they have linked to. This an important means by which individuals can keep track of what has happened to their personal information. Digest requirements would still apply to both Finance and DHS.

6.6 IPP 6 Access to personal information

IPP 6 requires an agency to allow an individual access to personal information it holds about them.

6.6.1 Finding

As with the current account linking system, users will be aware of much of the information that the GSE holds about them because they will have entered the information themselves via the internet to open their account and to establish a profile. Information about when an individual has conducted a transaction through the account will also be available through their australia.gov.au account. Information about the questions asked of an individual and the responses given will not be stored by the GSE or the Authentication Hub or DHS. As a result providing access to this information will have to be through audit logs and this will not be easy.

For privacy reasons outlined in the PIA on AGOSP, information held in the audit logs of the GSE and GSE Hub is not easy for anyone to access, including the individual. IIS considers that the privacy benefits of configuring the information in the log this way outweigh any privacy benefit from making the logs easier to access. However, if an individual considers they need access to more information than is already available through their australia.gov.au account they will be able to exercise their rights under Freedom of Information law to gain access to these logs.

On the information IIS has so far, it considers this is an appropriate balance to be struck.

6.7 IPP 7 – Keeping records relevant, complete, up to date and not misleading

IPP 7 requires an agency to take reasonable steps, by correcting, deleting or adding information, to ensure that, taking into account the purpose of collection, the personal information it holds is relevant, complete, up to date and not misleading. If an agency does not agree with an individual's request to amend or delete a record, it must (unless an exception applies) attach a statement made by the individual.

6.7.1 Finding

Apart from logging data and any analytical data, as with the current arrangements most of the personal information held in relation to the GSE provisioning service will be within the control of the individual who will be able to amend the information whenever they wish, and in whatever way they wish. Information provided to DHS via the GSE will be subject to the usual process of access and amendment via Freedom of Information Legislation.

6.8 IPP 8 Checking accuracy before use

IIP 8 requires an agency to take reasonable steps, taking into account the purpose for collecting, to check accuracy, completeness and currency of personal information before the agency uses it.

6.8.1 FINDING

In the case of the GSE question and answer process, the GSE will not check the accuracy of information that the individual has provided before conveying it to DHS. Neither would it check the accuracy of the information before acting on an individual's request to GSE to use profile information to populate an answer to a DHS question or to update GSE profile information from such an answer.

Taking into account the role of GSE as neutral service provider for DHS and the fact that it is a conscious privacy design feature to give individuals control over what information they provide to DHS, IIS considers that this arrangement in relation to GSE is appropriate.

However, IIS notes that GSE services have the potential increase the risks to an individual arising from inaccurate information holdings. This risk can be managed by high quality customer inquiry and complaints handling services and a strong focus on data quality at the initial point of collection. However this is primarily a DHS matter.

6.9 IPP 9 PERSONAL INFORMATION ONLY TO BE USED FOR RELEVANT PURPOSES

IIP 9 requires that an agency only use personal information it has collected for relevant purposes.

6.9.1 FINDING

At this stage, IIS is not aware of any intention at this stage to use the information collected by the GSE for purposes not relevant to the purposes outlined for establishing the new accounts provisioning process. There may be a risk of new purposes being implemented that are perceived by the community as unacceptable function creep. IIS discusses this in Section 8.3 of the report

6.10 IPP 10 LIMITS ON USE AND OF PERSONAL INFORMATION

It is a key privacy principle that once collected, information should only be used for the purpose for which it was collected. IPP 10 says that an agency that has collected information for a particular purpose should not use the information for any other purpose unless certain exceptions apply. These include:

- that the individual has consented to such other use; or
- the purpose is directly related to the original purpose of collection; or
- other public interest circumstances apply, for example, threats to health and safety, need to enforce the criminal law, protect public revenue, or it is authorised by law.

6.10.1 FINDING

IIS is not aware of any intention to use the information collected through the new provisioning process for purposes other than account provisioning purposes (either the person's australia.gov.au account or DHS master program online account).

However, there is a clear intention in the future to expand the uses for account provisioning processes to other agencies and for other information collection purposes. As mentioned in the previous section whether these changes are perceived as function creep rather than as desirable enhancements will depend on the process used to implement them. IIS discusses this in Section 8.3 the report.

6.11 IPP 11 LIMITS ON DISCLOSURE OF PERSONAL INFORMATION

IIP 11 places limits on the circumstances in which an agency can disclose the information it holds to another person, body or agency. It does not limit the purposes for which an agency can disclose such information as long as the relevant circumstances apply. These include:

- the individual is reasonably likely to have been aware, or made aware under IPP 2, that information is usually passed to that person, body or agency;
- the individual has consented to the disclosure; or
- other public interest circumstances apply, for example, threats to health and safety, need to enforce the criminal law, protect public revenue, or it is authorised by law.

6.11.1 FINDING

IIS is not aware of any intention to disclose the information collected by GSE in circumstances other than those where an individual will be aware of or have consented to the disclosure or other public interest circumstances apply.

To comply with IPP 11 GSE will, at the very least, need to ensure that individuals are made aware that their questions and answers will be disclosed to DHS and the relevant master program. However, as for uses discussed in the previous section, whether any proposed changes to disclosure and the basis on which it is made are perceived as function creep rather than as desirable enhancements will depend on the way such changes are implemented. IIS discusses this in Section 8.3 of the report.

7 KEY ISSUES FOR ACHIEVING TRUST

In addition to the risk of noncompliance with the Privacy Act, privacy issues in relation to the new provisioning process could arise from individuals fearing that they will lose control over their personal information or that the organisation will lose control over it. This can occur even where an initiative is compliant with privacy law. Concern can be driven by uncertainty about whether or not individuals can trust the entities to whom they give personal information, or who have control over it, to look after it and use it appropriately.

Research is also showing that whether individuals are prepared to trust an entity often depends on the risks of failure of any sort and who bears that risk when it occurs.

When governments or organisations develop new IT initiatives they very often focus on managing their own risks without regard for whether or not the risk is being shifted to the individual end user.

There is also an emerging view that excessive reliance has been placed on 'front end' mechanisms of end user control such as notice and consent to protect end user privacy.[2] This approach leaves end users bearing the risk in circumstances where they are not equipped, and as research is showing, not willing, to bear it.

[2] See for example "A New Approach to Trust and Privacy in the Information Age" – a paper for the Privacy and Trust Partnership conference convened in the Parliament House of NSW, Sydney, 4 July 2007, online at www.iispartners.com/white_paper.pdf

Reliance on consent can also be less effective in the government context where individuals may have little choice about providing personal information if they wish to receive essential benefits or services, or interact in other unavoidable ways, such as the payment of tax.

Major privacy issues can therefore arise through lack of concern about end user risk by organisations implementing new systems combined with heavy reliance on increasingly ineffective front end 'privacy protection' measures.

In addition, a key strategic priority for the new user provisioning service is to meet users' needs in their interactions with government. In seeking to implement a user focussed service it will be important to recognise that user requirements for identity management for e-enabled services between citizens and business and government are different from a security law or enforcement requirement. There is a risk that these separate requirements are blurred when implementing new IT systems. There is a risk if the differences are not recognised and managed that individual trust and the GSE's ability to meet user needs will be undermined.

8 OTHER POSSIBLE RISKS AND BEST PRACTICE ISSUES

The section identifies the key possible risks beyond compliance that can arise in relation to an initiative of this kind and then goes on to consider the extent to which, on the information IIS has so far, these arise in relation to the new account provisioning service. Where necessary, IIS makes a recommendation about how to address the issue.

8.1 RISK OF MAKING IT EASIER TO LINK INFORMATION ACROSS AGENCIES

A key privacy risk that could arise from the new provisioning service is that it might make it easier for information about an individual user to be more easily linked and aggregated across agencies participating in the service. There are two types of information that could be linked:

- existing information that each agency holds independently of the user provisioning system; and
- new information being generated by the new account provisioning process: namely user data trails about an individual's interactions with agencies.

The privacy risk increases if either or both of these types of information are able to be linked more easily across agencies to create a 'whole of government' picture of an individual's interactions with agencies.

8.1.1 PREVIOUS ASSESSMENT RELATING TO THE AUTHENTICATION HUB

In its December 2007 PIA report on AGOSP (now called the GSE) IIS examined the risk of linking in relation to the Authentication Hub which will play a critical role in the new account provisioning process. IIS identified that the Authentication Hub could be used to link information about an individual across agencies in a way not possible before, but that there are some very significant barriers in the way of this happening. These barriers include:

- that the Authentication Hub that does not hold personal information and is separate from the entities (agencies) holding personally identifiable account information;

- the use of MBUNs to link accounts rather than one identifier per user or a centralised map of agency identifiers;
- the separation of data trails generated by a user's interaction with the GSE Hub, from those created from interaction with the GSE (australia.gov.au) portal and with other agencies;
- very strict requirements on access to audit logs to connect end to end transactions, including the need for a court order for access.

IIS concluded that these features meant that linking information would require active collaboration between personnel in agencies and the administrators of the Hub as well as significant technical and administrative effort to put the information together in a significant way. Generally speaking these barriers would apply to those seeking to do this in either an authorised or unauthorised fashion.

Other features of an australia.gov.au account that, in some cases, could make linking less valuable to achieving a whole of government picture were that individuals:

- can have more than one australia.gov.au account;
- do not have to provide proof of identity to open an australia.gov.au account;
- have access to a range of channels to interact with government.

IIS identified a key vulnerability in the case where an individual's australia.gov.au account credential is compromised. Where the individual's credential is compromised, it is possible for an unauthorised individual to gain access to all of the accounts linked to the credential.

IIS concluded that, in the environment of that time of limited use and limited available additional information about individuals, these risks were manageable and acceptable.

However, it recommended that Finance should undertake a number of activities:

1. Continue to allow individuals to interact through a range of channels and to have multiple *australia.gov.au* accounts, including credentials of different strengths consistent with security threats and requirements as they evolve over time.
2. Not allow federation attributes (agencies and individual has linked to) to be included in authentication assertions to agencies.
3. Review the security controls to be placed around the MBUN and an individual's *australia.gov.au* account to ensure they are treated as having the same level of protection as personal information.
4. Implement mechanisms to ensure that the adequacy of the DHS infrastructure is revisited and strengthened as the capability of the AGOSP portal extends and the number of users expands. This includes monitoring the development of technologies that prevent linkage altogether and exploring the possibilities of deploying it as it becomes available and appropriate.
5. Review Centrelink's governance arrangements for the Authentication Hub and ensure that there are arrangements in place that give Finance adequate control over the business processes and policies that apply to the Hub.

6. Prepare a plan for increased appropriate separation of the Authentication Hub including logical separation, independent administration and independent governance arrangements. Depending on the outcome of the analysis necessary to prepare the plan, including the second and third PIAs physical separation might need to be considered.

Since the time of these recommendations, the governance arrangements for the Authentication Hub (now called the GSE Hub) have changed. Although DHS (through Centrelink) still operates the GSE Hub, Finance is the business owner of the Hub, and DHS operates it as a service provider to Finance. In addition, DHS no longer uses the GSE Hub for its own separate single sign-on authentication purposes.

8.1.2 Does the new provisioning process increase the risk of linking?

IIS assessed the features of the new provisioning process to identify whether there are any changes to the way the GSE Hub process works, or any additional aspects to the process, aside from the Hub that may increase the risk of linking and gaining a whole of government picture of an individual.

There are a number of features of the design which seek to minimise the risk of linking including:

- using the GSE Hub and an agency specific MBUN to enable a master program to link a question and answer response with an individual's online account;
- logical separation of the GSE Hub from the question and answer process mediated by GSE;
- ensuring that the GSE does not store in its data structure the specific questions asked of an individual or the answers they gave.

8.1.2.1 Interaction identifier

A new feature of the design is the addition of the interaction identifier to the messages travelling from end-to-end of the process starting with the question and answer process through to the point where DHS tells the Hub and the GSE notifies the individual that the process of provisioning and linking a master program online account is complete. (However, note that the individual does not see the interaction identifier). This feature could be used to more easily connect the various aspects of individual's transaction with the agency than was possible before. It would not have a direct impact on the ability of master programs (or agencies) to connect information across agencies because the interaction identifier is globally unique and not reused

IIS has concluded that having the interaction identifier is necessary in order for DHS to be able to connect a question and answer session with the MBUN that the Hub sends it for linking to the individual's online account. Indeed this requirement arises precisely because of the privacy driven design decision to mediate the linking through the Hub rather than directly between the GSE and DHS. This latter approach would have required the GSE and DHS to exchange either the individual's GSE MBUN or the individual's master program identifier which would have breached a key australia.gov.au design principle not to share agency identifiers.

IIS considers that ease with which the transaction identifier can be used for purposes other than to enable a master program to link a question and answer response session to the provisioning of an individual's online account have been diminished by the fact that neither the GSE nor the GSE Hub, nor DHS/master program stores the interaction identifier in their data structure once the provisioning process is completed. The interaction identifier will, however, be stored in each of the

GSE's, GSE Hub's and DHS' audit logs. This means that the interaction identifier could be used to connect the relevant parts of the transaction extracted from the GSE, the GSE Hub and the relevant master program in a way that was not possible before. However, this would still only be possible after the extensive technical and administrative barriers mentioned above have been overcome.

8.1.2.2 AGENCY REFERENCE NUMBER

Another new feature of the enhanced provisioning system is that through the activation code process an individual's ARN will be entered into the account provisioning system. This could increase the risk of linking across agencies. However, IIS understands that although the individual's ARN will therefore travel through the GSE, and may be held in memory, it will be very difficult to view and only downloaded into a data dump and saved as a file if it was necessary because, for example, there was a hardware failure. Even so, IIS understands it would be very difficult to read in this form. It will not travel through the GSE Authentication Hub at all, as it is only entered as part of the question and answer dialogue between the GSE and DHS.

8.1.2.3 FINDING

IIS finds that the interaction identifier as currently configured appears to create a relatively low level of addition to the risk. However, whether this remains the case may depend on the extent to which the current barriers are retained and adhered to. This in turn depends on the strength of the change management and governance processes for the GSE. Governance and change management including function creep are discussed in other sections of this report.

IIS also finds that the use of the ARN in the account activation code process does not increase the risk of linking as long as, as is currently the design, the ARN is not stored as a record in the GSE or GSE Hub and where it is held in memory, it is not easily accessible.

IIS has not identified any other features of the new provisioning process that might increase the risk of linking, at least between the GSE, GSE Hub and DHS.

IIS considers that there may be an increase in the risk of the linking of information between DHS master programs, depending on how the DHS part of the process is designed and implemented. However, IIS does not currently have any information about this at this stage. For example, if DHS has a central server that mediates between the GSE Hub and each of the master agencies, there could be a chance that the DHS server could have additional information that might enable linking of information about an individual across master agencies. IIS understands that DHS is conducting its own PIA on its part of the new account provisioning process and is outside the scope of this PIA.

However, as identified in IIS' 2007 PIA on australia.gov.au and the Authentication Hub, the overall risks of linking (unauthorised and authorised), both in terms of likelihood and impact will rise as a result of:

- increased use of the provisioning process and GSE services generally;
- increased value and rewards from linking the information both for government, potentially for individuals, and for any malicious outsider;
- gradual reduction in available channels as the online channel becomes increasingly dominant and the cost efficiency of keeping other channels available increases;

- as information collected through other channels potentially becomes available electronically (cf Whole of Government Reliance Framework).

As a result, IIS considers that the thrust of the recommendations it made in its 2007 PIA remain important to both the GSE Hub and the new account provisioning process. In particular, these relate to:

- ensuring the governance of the GSE Hub and the account provisioning process are regularly reviewed and commensurate with the privacy risks; and
- regularly reviewing the infrastructure used for achieving single sign-on.

As the move to whole-of-government interactions with individuals gain momentum the issue of governance will become an increasingly critical tool for addressing risk of linking information about individuals across agencies and gaining a whole of government picture of an individual. IIS discusses the question of governance and makes recommendations about this in Section 8.6.

On the question of infrastructure, IIS is aware that authentication technology is rapidly developing. The technology is moving away from federation of authentication from an organisation perspective (which tended to pay insufficient attention to user control and separation of parties) and towards a much improved user centric approach federation. Although the GSE Hub is a good early example of the latter, IIS considers that Finance should regularly monitor these newer developments and where appropriate incorporate them into its authentication infrastructure. This will be particularly important as GSE services develop and the GSE Authentication Hub becomes and increasingly critical part of an individual's whole-of-government interactions.

Recommendation 1 – Technology: Monitor and adopt best practice federated authentication technology

IIS recommends that Finance should monitor technology developments in the area of federated authentication that could further reduce the risks of linkage that arise from the use of the GSE Authentication Hub. Where practical and appropriate it should seek to adopt best practice technology as the Hub becomes an increasingly central part in whole-of-government online authentication.

8.2 Risk of use for purposes unrelated to account provisioning

IIS considers that there could be a risk that DHS might use the information from question and answer transactions for purposes unrelated to establishing PORO for an online account. As stated above, there does not appear to be any intention on the part of DHS to use the information for any other purpose. But there does not appear to be any technical barrier preventing DHS from using the information it receives through the question and answers for other purposes. For example, it could use information about address to detect that the individual has changed their address. Further, it might possibly use the information to make physical contact with them for some reason. These may or may not be legitimate in terms of the DHS program objectives or the terms and conditions on which the individual engages with a particular program. However, this would be a secondary purpose unrelated to the account provisioning process which the individual may not be aware of or have consented to.

Allowing DHS to use the information from questions and answers that should be designed purely to provision an account for purposes other than these this might undermine individual trust in the GSE account provisioning service and the integrity of the service overall.

This would be particularly so if the privacy notices provided by australia.gov.au say that the information will only be used for the account provisioning process when, in fact, DHS was using it for an unrelated purpose. The key to maintaining compliance with the Privacy Act and trust will be for Finance and DHS to ensure that privacy notices provided through the account provisioning process accurately reflect the purposes for which DHS is collecting personal information through the question and answer process.

IIS understands that the issue of how DHS uses the information is collects through the question and answer process is outside the control of Finance. As a result, IIS does not make a recommendation about this.

8.3 FUNCTION CREEP

IIS has discussed above the risk of linking information about an individual across agencies that could arise as a result of the new account provisioning process. The linking of information would be a change in purpose that may or may not be acceptable from a privacy point of view and may or may not be acceptable to the community.

It is also clear that the technology to provide the account provisioning service is being established with the explicit purpose in mind of extending the question and answer function to enable form filling and information provision for other purposes besides that of account provisioning. Whether or not such changes are acceptable and avoid being regarded as unacceptable function creep will depend very much on the process undertaken to implement such changes. In particular, it will be important to be able to identify when such changes are significant enough to warrant further privacy impact assessment and then to ensure that there is appropriate public scrutiny before a decision is made about whether or not to implement proposed changes.

8.3.1 FINDING

IIS notes that Finance and DHS have agreed a change management process. However, this appears to be geared more towards technical and operational issues of a relatively low level kind rather than towards major changes of policy or technology. Also, in the current change management process, the significance of change is assessed on the basis of such matters as cost and impact on the project, rather than privacy implications of any proposed change however IIS notes the inclusion of privacy as a field to be completed in the AGOSP Configuration Panel Request From (see Appendix D of Customer Support Processes for the Government Services Environment (GSE)).

IIS commends the fact that Finance has noted potential privacy implications arising from policy and service changes relating to the GSE and sought privacy impact assessments of them. However, as GSE services become more widely used it IIS considers it will be necessary to have a documented and more formal process for managing the impacts of privacy in relation to policy or major technological changes relating to the GSE.

IIS considers that the key planks to achieving an appropriate change management process that will prevent changes from being seen as unacceptable function creep are:

- a documented process for managing significant policy and associated significant technical changes to the GSE; and
- an independent governance process which includes community involvement.

Having a documented process helps to ensure that the agreed processes continue over time and do not slip away when there is change in personnel or the department is restructured. This is particularly helpful when more than one department is involved. Having independent community involvement ensures that changes are not just seen from each Department's perspectives but also have direct input from a consumer perspective. Being able to point to such a document can help to establish the process as trustworthy and also reassure consumers who may be concerned about arbitrary change.

In this regard, consumer emphasis on the importance of governance and change management in relation to the Personally Controlled Electronic Health Record and ongoing publicly expressed concerns about the lack of attention to it is worth noting.

The issue of governance for the GSE is discussed in Section 8.6.

Recommendation 2 – Business as usual: A documented process for identifying and managing major change having privacy implications

IIS recommends that Finance documents a process for identifying and managing privacy in relation to proposed major policy and technology changes to the GSE. The document should formalise the approach that where changes to the GSE are identified as having significant privacy implications the process should include a privacy impact assessment and a means for public scrutiny, including community consultation and potentially parliamentary scrutiny.

8.4 Risk of lack of transparency

IIS has discussed the notice requirements relating to IPP 2 in Section 6.2. Complying at a best practice level with notice requirements as outlined there will assist substantially in achieving transparency and individual user trust in the new account provisioning process.

There is also a wider issue of transparency relating to this initiative. There is a risk that there could be other underlying objectives relating to the initiative that agencies are reluctant to expose because they fear that individuals may be concerned about them and there may be a negative public reaction. These kinds of issues relate to the potential for streamlined government processes to facilitate and be used for government efficiency, revenue recovery, or law enforcement objectives. Agencies with these objectives in mind may seek to influence the design of a project without these reasons being publicly surfaced.

IIS has no evidence that this is the case. However, if there are any such hidden objectives, which may be quite legitimate, it will be absolutely critical that these are made explicit and factored into the public consultation on the initiative. There is nothing more fatal to individual and community trust in an initiative than the discovery, once a project is well under way, that there are objectives other than those publicly stated ones.

Also, if there are law enforcement or other efficiency or revenue raising objectives, it is important that the governance structures in place are commensurate with the increased privacy risks that a project with these kinds of objectives may raise.

As IIS has no knowledge of any such agenda on the part of any of the involved agencies or otherwise, IIS does not make a recommendation about this.

8.5 Safety-net and burden of risk

8.5.1 Customer support

A key risk where there are multiple parties involved in service provision is that when problems occur or the system fails there is no clear avenue for the individual to take to have the problem solved. The individual may be passed from agency to agency with no agency willing to take responsibility for solving the problem. This may arise particularly if solving the problem appears to require more than one agency to take action. Other concerns can be that customer service is not available at the times that the customer needs it.

Under current arrangements, Finance provides a service desk which is a first point of contact for users of GSE single sign-on services and is responsible for escalating incidents raised or questions asked to the responsible service provider or agency. The GSE service desk provides individuals via australia.gov.au with 24 hour online self-help support and a 'Contact Us' email facility which is actioned by service desk staff between 9.00am and 5.00pm Monday to Friday with 95% of all requests resolved or escalated within 8 business hours and 100% within 5 business days.

Where the GSE service desk cannot resolve the issue, the matter is escalated to a higher level either within the GSE or to the relevant service provider or agency where the matter is to be resolved. The service provider or agency is required to notify the GSE service desk when the matter is resolved.

The draft MOU between DHS and Finance for the new account provisioning arrangement appears to continue this arrangement. It also includes a requirement for:

- Customer support via email between 8am to 5pm provided by DHS;

8.5.1.1 DHS departmental support 365 days per year by phone. The phone service is to be available on week days for 21 hours per day and week end availability is 16 hours on Saturday and 18 hours on Sundays and public holidays. This provides a means for DHS customers to contact DHS directly by phone if they experience a problem with the account provisioning process. DHS will liaise with the GSE service desk if such coordinated response is required. The process includes a GSE incident manager who has overall responsibility for seeing that the process works well and is adhered to, and also a GSE problem manager who is responsible for managing the lifecycle of all problems.Finding

The documentation appears to provide for an adequately coordinated response and a means of monitoring centrally how well the process is working.

8.5.2 Terms and conditions

A further issue can be that the terms and conditions that an individual is required to agree to when the engage with a service are hard to read, and place an unfair burden of risk on the individual. Terms sometimes include statements that seek to remove any liability from the agency even when this is not strictly possible. It can also be the case that such terms do not explain the security

protections that the service or agency has in place or privacy reasons behind some of the terms and conditions.

8.5.2.1 FINDING

IIS understands that the current terms and conditions used for registering for australia.gov.au account will be retained. IIS has read these and considers that these remain appropriate in the light of the enhanced account provisioning process.

IIS understands that DHS will provide its own terms and conditions which will be presented at the time the person undertakes the enhanced account provisioning process. As a result, this is outside the scope of this PIA process and will be part of the DHS PIA process.

However, IIS considers that the current terms and conditions used by Medicare could not be considered best practice in this regard. https://www2.medicareaustralia.gov.au/pext/coin/termsAndConditions.do

IIS considers that the terms and conditions that Finance drafted for the initial release of single sign-on arrangements should be used as a model for terms and conditions to be used by DHS and Finance for the new account provisioning process. IIS understands that this is part of an agreed process.

8.5.3 DHS AUTOMATED DECISION MAKING

IIS considers that the DHS automated risk based question and answer process could raise some privacy issues. IIS comments on them briefly but recognises that they may be beyond the brief of this PIA to the extent that they do not impact on the GSE service. IIS considers that there is a possible risk that an individual could be unfairly discriminated against on the basis of information he or she provides in the automated risk assessment process. There is also a risk that an individual who is unsuccessful in establishing PORO or an online account with the master agency will not be able to find out the basis on which they were unsuccessful. This is largely a matter for DHS to address. However, where an individual is told during the account provisioning process that their question and answer session has been terminated and the account linking process unsuccessful, the GSE should ensure that the individual is told at the same time where he or she can get more information about the reason why the account provisioning process was unsuccessful. The process for getting more information should be readily accessible and user friendly. Ideally, there should be a review or appeal process. IIS assumes that individuals would be able to follow DHS' normal administrative review processes for this.

Recommendation 3 – Business-as-usual: Information about where to find out reasons for unsuccessful account provisioning process

IIS recommends that where an individual is told during the account provisioning process that their question and answer session has been terminated and the account linking process unsuccessful, the GSE should ensure that the individual is told where he or she can get more information about the reason why the account provisioning process was unsuccessful. The process for getting more information should be readily accessible and user friendly.

8.6 GOVERNANCE

IIS considers that a key principle should be that, in parallel with the development of seamless whole-of-government initiatives, there should be the development of seamless whole-of-government governance, which includes whole-of-government accountability and management of citizen risk.

On the question of the adequacy of the governance for the GSE Hub and the new provisioning process IIS finds that the introduction of the provisioning process and the resulting increased use of the GSE and the GSE Hub as providers of whole of government capable services justifies a strengthening of the governance arrangements. Currently Finance is the business owner of the GSE and Authentication Hub and DHS operates the Authentication Hub on behalf of Finance and there is a MOU between Finance and DHS in relation to the Hub. The proposed MOU covering the new account provisioning process sets out DHS requirements in relation to GSE services. These matters include the requirements for the Authentication Hub, the principles governing the relationship between DHS and Finance and their agreed roles and responsibilities.

The MOU also includes a change control process for both project and business-as-usual change requests relating to the GSE. These envisage the use of existing management structures to process and approve change requests. This involves using the Change Advisory Board (CAB) which meets regularly and is chaired by the GSE Change Manager and includes members from Finance and DHS and ad hoc stakeholders invited as necessary in relation to a particular change. CAB meets weekly to discuss technical and operational changes to the GSE Hub. The MOU allows for the possibility that the GSE Change Advisory Board may establish governance structures for particular GSE components which may have special powers.

IIS understands that should a significant policy or technical change to the GSE Hub be proposed the issue is considered by the Assistant Secretary of Finance online services and in most cases escalated to the Deputy Secretary for approval.

If the GSE Hub and associated services become increasingly the point of connection in individual whole-of-government interactions, as the Government appears to envisage, it becomes increasingly important that its governance is not principally the responsibility of just one government agency. IIS has not identified any evidence at all that the governance by Finance so far has been anything other than exemplary and conducted with due concern for the privacy and other interests of individual users.

However, IIS considers that it will be crucial to achieving long term individual user trust in the GSE including the Authentication Hub that its governance is seen as independent from any one particular agency so as to avoid any real or perceived issues of conflict of interest.

Further, IIS considers that as the Government seeks to simplify individual interactions with Government, including through merging the administrative and technical back ends of agencies such as is occurring with DHS and master programs, it will be important for there to be an independent citizen and consumer voice in decisions about policy and operation of the GSE and its services including the GSE Authentication Hub.

Independent and user/citizen inclusive governance will be a critical tool in addressing the risks IIS has identified above in relation to:

- preventing changes to GSE services and the Authentication Hub which amount to unwelcome function creep, such as linking information about individuals across agencies in ways that individuals to not expect and find unacceptable;

- ensuring coordinated seamless customer service and safety-net mechanisms;

- seamless whole-of-government approaches to accountability, transparency and information provision.

Recommendation 4 – Governance: Independent policy making body for GSE including Hub

IIS recommends that Finance take steps to implement a governance structure for the GSE including the GSE Authentication Hub that is independent from any one particular Australian Government agency. It should include:

- A CEO that is not part of a line agency structure of responsibility;
- A board with power to determine policy and make important operational decisions. The Board should have a mix of representatives from relevant government participating agencies and include a significant component of consumer / citizen representatives and a recognised privacy expert.