myGov and privacy – explanatory statement

The department manages the myGov online service on behalf of the Australian Government.

The myGov service became operational in late May 2013 and provides Australians with easy, fast and secure online access to a number of government agencies with one username and password.

The department takes the privacy of customer information seriously and an important element of the approach is to undertake rigorous and independent Privacy Impact Assessments of key services for which we are responsible. The first myGov release in May 2013 was subject to such a Privacy Impact Assessment to assess the privacy impacts of the myGov design and operation.

The Privacy Impact Assessment made six recommendations which the department agreed to and addressed prior to the implementation date, noting that a number require ongoing monitoring and action which is being undertaken. The recommendations are detailed in the *Executive Summary myGov (First Release) Privacy Impact Assessment May 2013.*

The *Introduction of myGov (First Release) Privacy Impact Assessment* describes the design and operation of the myGov service for the May 2013 release. Since that time, additional releases have occurred that may have modified the design and operation of the myGov service as documented in the *myGov (First Release) Privacy Impact Assessment.*

Department of Human Services introduction of myGov (First Release)

Privacy Impact Assessment

8 May 2013

HWL EBSWORTH
LAWYERS

Table of Contents

Executive Summary

1. myGov Overview

1.1 The Australian Government's primary online entry point is australia.gov.au. It provides access to government information and services for individuals. It includes, among other things, a single sign-on service, allowing people to visit multiple government websites without repeatedly signing in at each site.

1.2 The myGov project is part of the Australian Government's investigation of ways to improve individuals' ease of use and access to Australian Government services. The Department of Human Services (**DHS**) will assume the lead role in implementing the myGov project.

1.3 The myGov project involves:

- DHS creating a new myGov website;
- the Department of Finance and Deregulation (**Finance**), as manager for australia.gov.au, transferring management responsibility to DHS for authentication services that are currently performed as part of the australia.gov.au website (and which upon transfer will be performed as part of myGov). These authentication services are concerned with implementing processes and technology to allow account users to be authenticated and identified as the owner of an account. The authentication services include:
  - (i) management of the Authentication Hub; and
  - (ii) provision of user functions such as account registration, login, establishing Proof of Record Ownership and linking to Member Services; and
- DHS providing, over time, additional services to myGov users such as allowing individuals to communicate updated details to multiple agencies simultaneously and the ability for the individual to view all their government communications in one place.

1.4 Finance will remain responsible for the public content of australia.gov.au and the unauthenticated entry point for access to australia.gov.au. The australia.gov.au website will provide a link to allow users to navigate to the myGov website.

1.5 Enhancements and improvements to myGov will be implemented in a number of releases (**Releases**) over time.

1.6 The first release (**First Release**) involves:

- the creation of myGov in May 2013;
- the transition from australia.gov.au to myGov of authentication services which allow users to be authenticated and identified as the owner of an account; and
- the implementation of new user name recovery functionality.

1.7 The First Release also involves Finance transferring responsibility to DHS for information held in anonymous australia.gov.au accounts that do not contain, or refer to, the user's name or identity. The information held in these anonymous australia.gov.au accounts cannot be linked to an individual whose identity is apparent, nor is the information sufficient to be able to reasonably ascertain the account holder's identity. The information contained in the anonymous australia.gov.au accounts is described in more detail at paragraph 2.3 of Part 1 of this PIA.

1.8 All other existing australia.gov.au processes for creating an account and linking to Member Services will remain unchanged until further enhancements are introduced. A user's decision to link a myGov account to a Member Service and undertake the required proof of record ownership (**PORO**) process is entirely voluntary.

1.9 Post transfer, from Finance to DHS, of management responsibility for authentication services, DHS will continue to collect the same non-identifiable information as was collected by Finance. However, DHS will also collect, from users, their email address and mobile phone number. DHS will collect the email addresses and mobile phone numbers of users to support the introduction of the new user name recovery functionality.

1.10 The processes for storage and use of information in myGov remain the same as those that apply in australia.gov.au. Further, all security measures which are in place to protect user information within the australia.gov.au platform will be replicated in the myGov platform.

1.11 Importantly, individuals will not be 'forced' to use myGov or create a myGov account to access Australian Government services. Users will be able to access Member Services using face to face or telephone channels.

1.12 DHS has engaged HWL Ebsworth Lawyers to conduct a privacy impact assessment on the initiative to establish myGov. This Privacy Impact Assessment reviews the impacts on personal privacy arising from the First Release.

2. Findings

2.1 The First Release of the myGov project does not give rise to any new or heightened privacy risks that cannot be mitigated by the recommendations in section 3 below.

2.2 A high level analysis of the First Release compliance with the APPs was also undertaken, even though the APPs will not apply until 12 March 2014. No compliance issues (in addition to those discussed in relation to the IPPs) were identified. However, as myGov collections, uses and disclosures will be materially altered by subsequent Releases, myGov compliance with the APPs must be reviewed closer to the introduction of the APPs.

3. Recommendations

3.1 This Privacy Impact Assessment makes the following recommendations:

Recommendation 1 – implement processes including privacy audits and additional privacy impact assessments to monitor and manage privacy issues arising from myGov and subsequent Releases	
Further Releases of myGov will involve materially different collections, uses and disclosures of personal information to those occurring under the First Release. DHS should undertake additional privacy impact assessments (or produce addendums to this PIA) to assess the privacy impacts of each additional Release, once the technical details and processes of those Releases are better known. DHS is also encouraged to provide additional privacy assurance by arranging for regular privacy audits of myGov to be conducted.	
Department Response	Agreed. DHS will undertake additional PIAs and/or addendum PIAs as the myGov service develops further enhancements and improvements to the system. DHS will also arrange for regular privacy audits to be conducted on the myGov system and services.

Recommendation 2 – implement processes to monitor and manage privacy issues arising from myGov function creep	
DHS should implement processes and governance arrangements to ensure that function creep does not occur in an unmonitored manner.	
Department Response	Agreed. DHS addresses issues of function creep in the myGov project by having a governance framework with external representatives that oversees each stage of the project. The Reliance Framework Board includes representatives from the Australian Tax Office, the Attorney General's Department, the Department of Finance and Deregulation and the Department of Health and Ageing. The Board meets on a monthly basis and is responsible for managing the project including developing the program plan. It is also tasked with providing biannual reports to the Secretaries ICT Governance Board.

Recommendation 3 – include the Privacy Statement at Attachment B to this PIA on the myGov website. The Privacy Statement reflects the technical details of the First Release, including that DHS now manages myGov.	
This PIA recommends that DHS includes the Privacy Statement at Attachment B on its myGov website. DHS manages myGov on behalf of the Australian Government and the Privacy Statement at Attachment B reflects DHS' record keeping in its capacity as the manager of myGov. The Privacy Statement complies with DHS' obligations under the Privacy Act. The Privacy Statement will need to be amended to address further Releases of myGov. If further Releases do not proceed, the statement will still need to be updated to address the introduction of the APPs on 12 March 2014. The Medicare, Centrelink and Child Support programs, delivered by DHS, are also Member Services which will rely on myGov to deliver their online services. Each of the Member Services will continue to display a privacy statement that is relevant to their particular service.	
Department Response	Agreed. DHS will include the Privacy Statement at Attachment B to this PIA on its myGov website. Additionally, a PIA or addendum PIA and updated Privacy statements will be drafted for each Release of myGov and it will be clear in the privacy statement that the statement applies to DHS in its record keeping capacity as the manager of myGov.

Recommendation 4 – address the use of myGov by authorised representatives of account users	
This PIA recommends that DHS provide users with instruction as to when a person can create and use a myGov account on behalf of another person. To this effect, DHS should include a statement in the terms of use on the myGov website that agents and representatives who create or use a myGov account to access another person's account with a Member Service must have legal authority to act for that other person. The exact words of this statement will depend on the myGov website technical explanation of how authorised representatives can use myGov when acting on behalf of another person.	
Department Response	Agreed. A statement will be placed in the terms of use and information placed on the myGov website that explains the responsibilities of the account user ensuring that authorised representatives rely on the arrangements that they have made with the Member Services in relation to using online services on behalf of another person.

Recommendation 5 – prepare terms of use that are consistent with Privacy Statement and myGov user instructions	
The myGov terms of use should be drafted to be consistent with the myGov Privacy Statement and the myGov user instructions.	
Department Response	Agreed. The terms of use will be reviewed prior to insertion in myGov to ensure that they are privacy compliant.

Recommendation 6 – explain to users how information they previously provided to Finance will now be managed by DHS	
Although there is no disclosure of personal information by Finance to DHS upon transfer of responsibility and although DHS will use the information collected under australia.gov.au for the same purposes, DHS should, as a matter of good management practice, explain to users that information users previously provided to Finance will now be managed by DHS. A statement to the following effect should be included in the myGov user instructions: "The australia.gov.au authenticated service has been upgraded to the myGov service. This upgrade is part of the Australian Government's myGov project to investigate ways to improve individuals' ease of use and access to government services. Previously, the Department of Finance and Deregulation managed the australia.gov.au authenticated service, with the Department of Human Services assisting as its service provider. The Department of Human Services will now take full management responsibility for the provision of authenticated services through myGov. The transfer of management responsibility from the Department of Finance and Deregulation to the Department of Human Services will not involve the transfer of responsibility for any personal information. This is because all australia.gov.au accounts, for which DHS will become responsible, are anonymous accounts and the information held in these anonymous australia.gov.au accounts cannot be linked to an individual whose identity is apparent, nor is the information sufficient to reasonably ascertain the account user's identity. The information that you provided to australia.gov.au will be used by the Department of Human Services for the same purpose as it was used by the Department of Finance and Deregulation."	
Department Response	Agreed. australia.gov account users will be provided with information about how the personal information that they provided to the authenticated austraslia.gov site will be managed by DHS. Essentially account users will be advised that no personal information that was provided to australia.gov has been provided to myGov.

Part 1 – Project Description

1. Purpose of the myGov project

1.1 Currently, individuals can create an online australia.gov.au account that has a single sign-on service and is linked to accounts the individual holds with any of the following participating programs or agencies:

- the Department of Human Services' Centrelink program, Medicare program and Child Support program;
- the Department of Health and Ageing's eHealth program; and
- the Department of Veterans' Affairs,

(referred to in this PIA as "**Member Services**").

1.2 Additional Australian Government agencies may become Member Services at a later date.

1.3 The myGov project will transition existing australia.gov.au accounts to myGov accounts and will offer additional services to improve ease of use and access to Australian Government services. In the First Release an additional service will be included that gives the account user the capacity to recover their user name by providing their email address or mobile phone number.

1.4 In order to understand how the transition from australia.gov.au to myGov impacts on personal privacy this PIA:

- first examines the initial transition from australia.gov.au accounts to myGov accounts; and
- then examines the impact of the user name recovery functionality.

2. Project Description: initial transition of authentication services from australia.gov.au to myGov

2.1 From May 2013 all existing australia.gov.au accounts (including existing links to Member Services) will be transitioned to myGov. Apart from the name change and significant useability improvements, the only change to australia.gov.au accounts will be the introduction of a user name recovery service.

2.2 The initial transfer of responsibility for managing australia.gov.au accounts from Finance to DHS will involve Finance transferring to DHS responsibility for information that Finance has previously collected from, or generated in relation to, account users for the purposes of administering australia.gov.au accounts. This administration covers the functions of australia.gov.au account registration, account login and linking the australia.gov.au account to the Member Services. From the time of transfer of responsibility, australia.gov.au accounts will no longer exist.

2.3 Finance will transfer the following information that remains relevant to the continuing operation of myGov. DHS will continue to collect information of this nature in its operation of myGov. For each account, this information will consist of:

- a non-identifiable user name (eg My Account XH123789) and user password;

- secret questions and answers provided by the user and that, if answered correctly, enable the user to access their account;

- the Member Services that the account has linked to it;

2.7 All australia.gov.au account users are anonymous (that is, their name does not appear on or in their account and the account does not contain information that would enable the account user to be identified).[1] DHS has confirmed that the secret questions and answers provided by the user cannot be used to identify any account user. They are merely a set of unverified questions and answers that cannot be attributed to a known or identifiable account user. DHS is unaware of any instance where a set of secret questions and answers has revealed the identity of an account user.

2.8 DHS will maintain or host myGov accounts using a combination of existing and new applications and infrastructure. Existing australia.gov.au Authentication Hub applications and new myGov applications will be deployed to new physical server hardware to provide the latest high performance, availability and security capabilities. New dedicated network and gateway infrastructure will provide integration and connectivity between Authentication Hub, myGov and associated system components. Existing infrastructure supporting the Authentication Hub data stores will be reused to enable transition from australia.gov.au to myGov without having to transfer user and Member Services information.

[1] The Authentication Hub was specifically designed so that it does not need to collect personal information.

2.10 Upon transitioning australia.gov.au accounts to myGov accounts, existing account users will only be able to access their new myGov account by:

- providing an email address and optional mobile phone number for SMS, which will be used to deliver the new user name recovery service;
- selecting three secret questions and providing answers; and
- agreeing to the new myGov terms of use.

2.11 Under the current australia.gov.au arrangements a user has to create a new account if they forget their user name. User feedback has supported the introduction of a user name recovery function. The user name recovery service will allow an account user to obtain their user "name" if they have forgotten it. Account users will be required to uniquely identify their account and prove ownership of that account before the user name associated with that account will be provided to them.

2.12 Upon transition from australia.gov.au to myGov, DHS will:

- take responsibility, from Finance, for user accounts and associated Audit Logs which will consist of de-identified information (non-personal) information;
- collect from all users, when they first use their myGov account, the user's email address or mobile phone number; and
- undertake, authentication of account users seeking to link their myGov account to accounts held with any of the Member Services.

2.13 DHS already, under australia.gov.au, undertakes the authentication (or account provisioning) service as a service provider on behalf of Finance. The "business as usual" authentication (or account provisioning) service provides individuals with the ability to prove ownership of a Member Service record through a question and answer process mediated through the individual's myGov account and the Government Services Environment (managed by DHS).

2.14 The Member Service will provide the Authentication Hub, managed by DHS, with a list of pre-set possible questions that individuals might be asked to establish proof of record ownership (**PORO**).

2.15 All other existing australia.gov.au processes for creating an account and linking to Member Services will remain unchanged in myGov until further enhancements to myGov are introduced. Further, all security measures which are in place to protect user information within the australia.gov.au platform will be replicated in the myGov platform.

Part 2 – Analysis of Release 1 compliance with Privacy Act

1. Assessment of compliance with IPPs and APPs

1.1 Each collection, use and disclosure of personal information under Release 1 must be assessed against the IPPs which apply until and including 11 March 2014. Attachment A includes a high level analysis of each IPP to confirm whether the IPP applies in Release 1. The analysis recognises that under Release 1:

- no personal information is transferred from Finance to DHS upon handover of responsibility for australia.gov.au authentication services;
- only a limited category of personal information is collected (after the transfer of responsibility from Finance to DHS); and
- no disclosures of personal information are planned.

1.2 Where the high level analysis in Attachment A has identified potential compliance issues and recommended actions, the issue has been fully explored in this Part 2. Accordingly, Part 2 only discusses key issues (and key or directly relevant IPPs).

1.3 A high level analysis of the First Release compliance with the APPs has been undertaken. No compliance issues (in addition to those discussed in relation to the IPPs) were identified. However, as myGov collections, uses and disclosures will be materially altered by subsequent Releases, myGov compliance with the APPs must be reviewed closer to the introduction of the APPs.

2. Transfer of authentication service responsibility from Finance to DHS

2.1 At the point myGov commences operation, DHS will assume management responsibility for information previously collected by Finance in its administration of the australia.gov.au authentication services. It is therefore necessary to analyse first whether the information collected by Finance is actually personal information which is regulated by the Privacy Act. If the information is personal information it will be necessary to analyse whether the disclosure by Finance to DHS of that personal information complies with the Privacy Act, and specifically IPP10 or IPP11.

Is the australia.gov.au account information personal information?

2.2 All australia.gov.au account users are anonymous as account user "names" consist of a combination of numbers and letters that do not identify the individual. The accounts hold only a limited amount of information (described in paragraph 2.3 of Part 1) which DHS cannot use to identify the individual account user.

2.3 As the information originally collected by Finance is not personal information, it is not necessary to analyse whether the transfer by Finance to DHS of responsibility for that information complies with the Privacy Act, and specifically IPP11.

3. DHS use of information originally collected by Finance

3.1 Although, the information originally collected by Finance for the purpose of creating an account in australia.gov.au is not personal information, and not subject to the Privacy Act, if there was personal information there would be no issue under IPP10 because DHS' use of that information will be the same as Finance's original use (and purpose of collection). Specifically Finance's use was to enable users to establish an online account to link to, and access, Member Services and DHS' use is the same.

3.2 Although there is no disclosure of personal information by Finance to DHS upon transfer of responsibility and although DHS will use the information collected under australia.gov.au for the same purposes, DHS should, as a matter of good management practice, explain to users that information users previously provided to Finance will now be managed by DHS. This approach will assist users to understand the evolution of australia.gov.au to myGov and the purpose of the collection and use of personal information upon the introduction of myGov.

3.3 Accordingly, it is recommended that a statement to the following effect be included in the myGov user instructions:

> The australia.gov.au authenticated service has been upgraded to the myGov service. This upgrade is part of the Australian Government's myGov initiative to improve individuals' ease of use and access to government services. Previously, the Department of Finance and Deregulation managed the australia.gov.au authenticated service, with the Department of Human Services assisting as its service provider. The Department of Human Services will now take full management responsibility for the provision of authenticated services through myGov.
>
> The transfer of management responsibility from the Department of Finance and Deregulation to the Department of Human Services will not involve the transfer of responsibility for any personal information. This is because all australia.gov.au accounts, for which the Department of Human Services will become responsible, are anonymous accounts and the information held in these anonymous australia.gov.au accounts cannot be linked to an individual whose identity is apparent, nor is the information sufficient to reasonably ascertain the account user's identity.
>
> The information that you provided to australia.gov.au will be used by the Department of Human Services for the same purpose as it was used by the Department of Finance and Deregulation.

4. Post transition collection, use and disclosure of personal information

4.1 Post transition, DHS will continue to collect the same information as Finance collected to perform the australia.gov.au authentication services. DHS will commence collection of a new category of information in the form of user email addresses or mobile phone numbers. This information will be stored in the user's account. An email address may, in fact will often, identify an individual, even if the address is stored in an anonymous account. By identifying the account user information that was previously not able to be linked to an individual may be capable of being linked to that individual and may become personal information.

4.2 DHS will use the email address to send an account user's user name to that account user on account creation. DHS will also use the email address and mobile number to send an account user's user name to that account user if that person notifies DHS that they have forgotten that information. This functionality will address australia.gov.au limitations which require a user to create a new account if they forget their user name.

4.3 DHS will not disclose the email address or mobile phone number as part of the First Release. DHS will only use the email address or mobile phone number as outlined in paragraph 4.2. Accordingly, the email address and mobile phone number will only be 'revealed' to the person who provided the information (and to whom the information relates). This is not a disclosure under the Privacy Act.

4.4 DHS will need to take steps to ensure that its collection of all existing categories of information and user email addresses complies with IPP1, IPP2 and IPP3. As analysed in Attachment A, the collection complies with IPP1 because:

(1) The collections of information from individuals are:

- for the lawful purpose of administering services provided by Australian Government agencies; and
- directly related to DHS' function of providing those services.

(2) Users will be notified of the meaning and implications of the collection of their

information in the short and long form Privacy Statement and will only be required to provide the personal information if they wish to use or open a myGov account. Accordingly, the consent to the provision (collection) of the personal information (which will occur when the user provides the information) will be genuine informed consent. Therefore, the collections are not by unlawful or unfair means.

4.5 As analysed in Attachment A, the collection complies with IPP3 because the collection of the personal information is:

- relevant to the purpose of collection, because it relates to creating an account in myGov and the user name recovery functions;
- up to date;
- complete; and
- will not unreasonably intrude on the affairs of the individual because it is provided by consent, held securely, and its use will be strictly limited to the purpose of collection.

4.6 DHS' collection and use will comply with IPP2 if DHS notifies the individual of the purpose of the collection. The Privacy Statement at Attachment B includes the notices that are necessary to ensure that DHS complies with IPP2. (This general requirement will also apply under APP5 which requires DHS to notify or make the individual aware of how and why personal information is, or will be, collected and how DHS will deal with that personal information.)

5. Storage and security of information

5.1 IPP4 requires DHS as the record-keeper to ensure that the record (the myGov account) is protected by reasonable security safeguards against loss, unauthorised access, use, misuse, modification or disclosure.

5.2 DHS will replicate, with some upgrade, the security features of australia.gov.au in the myGov platform. The myGov platform will comply with applicable security measures set out in the Australian Government Information Security Manual produced by the Defence Signals Directorate.

5.3 The security measures for ensuring the account is secure include storing data at a secure facility and recording when the account is accessed. Data in transit between myGov and Member Services is encrypted. There are no known security breaches concerning the information held in australia.gov.au. These measures have been assessed by DHS as sufficiently secure in light of nature of the information held.

6. Business as usual conduct of authentication services

6.1 There are two ways in which an account user can link to a Member Service - Options 1 and 2 described below. A Member Service may require that a particular option be used, but in the absence of such a requirement then a user may choose which option they use.

Option 1

6.2 The authentication and linkage of accounts process will involve the individual logging into a myGov account and then being transferred to the Member Service's landing page to undertake the authentication process.

Option 2

6.3 DHS will provide the Authentication Hub which, with information provided by the Member Service, will generate possible questions that individuals might be asked to establish

PORO. The PORO questions and answers contain information which can be attributed to a known individual as the questions are generated from a Member Service account where the account user is a known individual. This process will involve DHS collecting personal information from a Member Service or, where DHS is the Member Service, using information it already holds. The PORO questions and answers are stored by the Member Service.[2]

6.4 DHS, in its capacity as manager of the Authentication Hub will not use the personal information other than to assist the Member Service to establish whether or not an individual myGov account user owns a particular Member Service customer record and to facilitate the account linking process.

6.5 DHS, as manager of the Authentication Hub, will hold Audit Logs as described in paragraphs 2.4 and 2.6 of Part 1.

6.6 DHS will need to take positive steps to ensure that its collection of personal information from a Member Service (and the corresponding disclosure by that Member Service) complies with IPP2 – the Member Service has taken reasonable steps to ensure that the individual is aware of the purpose of collection and the entities to whom the collector will usually disclose the personal information. (This general requirement will also apply under APP5 which requires DHS to notify or make the individual aware of how and why personal information is, or will be, collected and how DHS will deal with that personal information.)

6.7 The decision to link a myGov account to a Member Service and undertake the required PORO process is entirely voluntary. DHS' collection of personal information from Member Services (and the Member Services disclosure) will comply with IPP2 if DHS notifies the individual of the fact that DHS will use the information to assist in the PORO process. The Privacy Statement at Attachment B includes the notices that are necessary to ensure that DHS and the Member Service comply with IPP2.

6.8 DHS' use of personal information will comply with IPP2 by virtue of the fact the authentication process will make it clear that participation in the authentication process will require DHS to undertake a fresh collection of personal information (collection of answers). Again, the individuals' participation will be voluntary and the uses and collections of personal information, consent based. Importantly, individuals will not be 'forced' to use myGov or create a myGov account to access Australian Government services. Users will be able to access Member Services using face to face or telephone channels.

7. Authorised representatives

7.1 Each Member Service will determine whether it will allow authorised representatives to use myGov on behalf of another person to access that other person's account. DHS should include a statement on the myGov website to the effect that authorised representatives must have authority to act. The exact words of this statement will depend on what other technical description the myGov website includes on how authorised representatives can or should create myGov accounts.

[2] The PORO questions and answers differ from the secret questions and answers provided by the user to australia.gov.au or myGov to enable the user to access their account because the secret questions and answers cannot be linked to a known user (they are held in an account which does not have an name which identifies an individual);

8. Sign off

8.1 HWL Ebsworth has prepared this Privacy Impact Assessment in consultation with DHS and has taken into account feedback received from the Office of the Australian Information Commissioner. HWL Ebsworth has relied on DHS for the description of the myGov project and has drafted the Privacy Impact Assessment on the assumption that the description of the project accurately reflects the handling of personal information.

8.2 HWL Ebsworth is of the view that the First Release of the myGov project does not give rise to any new or heightened privacy risks that cannot be mitigated by the recommendations set out in paragraph 3 of the Executive Summary.

Glossary

Acronyms	
APP	Australian Privacy Principle
DHS	Department of Human Services
DoHA	Department of Health and Ageing
IPP	Information Privacy Principle
PIA	Privacy Impact Assessment
POI	Proof of Identification
PORO	Proof of Record Ownership (see definition below)

Definitions	
account or account user	is synonymous with the concept of a security identity specific to a particular domain. The domains dealt with in this PIA are the Authentication Hub and Member Services using the Authentication Hub. In terms of australia.gov.au and myGov, the account is the same
Audit Log	A chronological record of system activities. Includes records to system accesses and operations performed in a given period
australia.gov.au	The branded online entry point for the Australian Government
Authenticate	The process of identifying a user using a credential e.g. user name, password, secret question and answer. A user must authenticate to myGov to access their myGov account. A user must authenticate to a Member Service website when linking to that Member Service using an existing Member Service online account.
Authentication Hub	The Authentication Hub provides services and interfaces for Authentication, registration and single sign on to online services for Member Services
Finance	Department of Finance and Deregulation
function creep	The incremental expansion in the purpose of a system, to a point where information is used for purposes not initially agreed to or envisaged and unrelated to its original intent. Such expansion is generally organic in nature and lacks overall direction, planning or oversight
Government Services Environment	Previously called the Australian Government Online Service Point (AGOSP)
Member Services	• the Department of Health and Ageing eHealth program; • the Department of Human Services' Centrelink program, Medicare program and the Child Support program); and • the Department of Veterans' Affairs
myGov	Unauthenticated 'public' content and primary landing page/entry point for myGov creation, account management, myGov services and access to myGov account services

myGov account	The authenticated portion of myGov containing an individual's security account, profile and service offerings e.g. myinbox, Tell Us Once
National e-Authentication Framework	A framework published by the Australian Government Information Management Office of the Department of Finance and Deregulation to provide a consistent, whole-of-government approach to managing identity-related risks
personal information	has the meaning given to it by section 6 of the Privacy Act
Privacy Act	the *Privacy Act* 1988
Proof of Record Ownership	The process used to establish a degree of confidence about the ownership of a user's record. This involves answering a set of shared knowledge questions or proof of identity questions. A user can choose or may be required by a Member Service to undertake this process when linking to a Member Service.

Department of Human Services introduction of myGov (Release 1)

Privacy Impact Assessment

Attachment A – IPP Compliance

8 May 2013

HWL EBSWORTH
LAWYERS

Table of Contents

Attachment A – Release 1 IPP Compliance

Below is a summary of key elements of the IPPs that are relevant to the analysis of Release 1 of the myGov project. The summary does not cover all elements of the IPPs and should not be relied on as a transcription of the IPPs.

In analysing the application of the IPPs, it is important to note that the information originally collected by Finance for the purpose of providing australia.gov.au, and then transferred to DHS to provide myGov services, is not personal information (and accordingly not regulated by the Privacy Act). This is because accounts are held in non-identifiable names and, until the collection of email addresses by DHS post transition to myGov, will not be attributable to an individual whose identity is apparent, or can reasonably be ascertained.[1]

1. IPP 1 – Manner and purpose of collection of personal information

1.1 The collection of personal information must be:

- for a lawful purpose; and
- directly related to, and necessary for, a function or purpose of the collector.

1.2 The personal information is not collected by unlawful or unfair means.

Analysis of compliance with IPP1

1.3 DHS' collection of personal information complies with IPP1 for the reasons set out below.

1.4 The collections of information from individuals are:

- for the lawful purpose of administering services provided by Australian Government agencies; and
- directly related to DHS' function of providing those services.

1.5 Users will be notified of the meaning and implications of the collection of their information in the short and long form Privacy Statement at Attachment B and will only be required to provide their personal information if they wish to use or open a myGov account. Accordingly, the consent to the provision (collection) of the personal information (which will occur when the user provides the information) will be genuine informed consent. Therefore, the collections are not by unlawful or by unfair means.

2. IPP2 – Solicitation of personal information from individual concerned

2.1 The collector must take reasonable steps (before or, if necessary, after collection) to ensure that the individual concerned is aware of:

- the purpose for which the information is collected;
- the fact (if this is the case) that the collection is authorised or required by law; and
- the entities to which the collector will usually disclose the personal information.

[1] ***personal information*** means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Analysis of compliance with IPP2

2.2 DHS complies with IPP2 for the reasons set out below.

2.3 The collection of email addresses will result in the collection of personal information where the email address identifies the individual who provides the email address.

2.4 Under IPP2 the notification must be provided before or at the time of collection, or if that is not practicable, as soon as practicable after collection. DHS will comply with IPP2 if it includes an IPP2 Notice, visible to users, on the myGov website in the form of the notice at Attachment B to this PIA.

2.5 The IPP2 Notice will be visible to the user prior to the point of creation of the myGov account and will consist of a short notice, with a link to a longer and more detailed notice. The long notice will be linked to the myGov terms of use and will be available in the privacy tab on the myGov website at all times.

3. IPP3 – Solicitation of personal information generally

3.1 The collector must take reasonable steps to ensure that the collection of the personal information:

- is relevant to the purpose of the collection, is up to date and complete; and
- does not unreasonably intrude upon the personal affairs of the individual.

Analysis of compliance with IPP3

3.2 DHS complies with IPP3 for the reasons set out below.

3.3 The collection of personal information under Release 1 (an email address) is:

(a) relevant to the purpose of collection, because it relates to creating an account in myGov and the username recovery function;

(b) up to date;

(c) complete; and

(d) will not unreasonably intrude on the affairs of the individual because it is provided by consent, held securely, and its use will be strictly limited to the purpose of collection.

4. IPP4 – Storage and security of personal information

4.1 The record-keeper must ensure that the record is protected by reasonable security safeguards against loss, unauthorised access, use, misuse, modification or disclosure.

Analysis of compliance with IPP4

5. IPP5 – Information relating to records kept by the record-keeper

5.1 The record-keeper must take reasonable steps to ensure that individuals are aware of:

- the types of personal information about them that are held by the department;
- the main purposes for which the information is used; and
- the steps the person should take should they wish to access their records.

Analysis of compliance with IPP5

5.2 The IPP2 Notice will also cover the matters required by IPP5. The IPP2 Notice should be drafted to only apply to DHS record keeping in its capacity as the manager of myGov. That is, the Notice should not confuse DHS' collections under myGov with DHS' collections for the purposes of the Centrelink, Medicare or Child Support programs, or for its other administrative programs.

6. IPP6 – Access to records containing personal information

6.1 The record-keeper shall ensure that individuals are entitled to access their records unless the record-keeper is authorised by law to refuse such access.

Analysis of compliance with IPP6

6.2 DHS' IPP2 Notice notifies individuals that they may gain access to their personal information and indicates an intention on the part of DHS to provide that access unless authorised by law to refuse to do so.

7. IPP7 – alteration of records containing personal information

7.1 The record-keeper shall take reasonable steps (by way of amendments to records) to ensure that the record is accurate, and not misleading, having regard to the purpose for which the information was collected or is to be used.

Analysis of compliance with IPP7

7.2 The personal information collected under Release 1 is of a very limited nature. Users will be able to update information provided (their email address) so records can be kept accurate. User email addresses collected by DHS may be updated by users provided the email address remains unique. Otherwise, it is difficult to see how IPP7 will apply in any practical way to Release 1. Accordingly, there is nothing to indicate that DHS will fail to comply with IPP7.

8. IPP8 – Record-keeper to check accuracy of personal information before use

8.1 The record-keeper shall not use information without taking reasonable steps to ensure that it is accurate, up-to-date and complete.

Analysis of compliance with IPP8

8.2 DHS will use personal information (email address) provided directly by the individual concerned. The collection from the individual concerned constitutes reasonable steps to ensure the accuracy and completeness of the information. Accordingly, Release 1 complies with IPP8.

9. IPP9 – personal information to be used only for relevant purposes

9.1 The record-keeper shall not use personal information except for a purpose to which the information is relevant.

Analysis of compliance with IPP9

9.2 DHS will only use an individual's email address for account creation and the user name recovery function. This is a relevant purpose and accordingly, Release 1 complies with IPP9.

10. IPP10 – limits on use of personal information

10.1 The record-keeper shall not use information for any purpose (other than the purpose for which it was collected) unless:

- the individual concerned has consented to the use of the information for that other purpose;
- the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
- use of the information for that other purpose is required or authorised by or under law;
- use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
- the purpose for which the information is used is directly related to the purpose for which the information was obtained.

Analysis of compliance with IPP10

10.2 DHS will comply with IPP10 if it uses the personal information only for the purpose for which it was collected, or if not used for that purpose then provided one of the exceptions listed above applies.

10.3 DHS should not use the personal information for any new or alternative purpose unless it first obtains legal advice that confirms that the new or alternative purpose is authorised under the Privacy Act.

11. IPP11 – limits on disclosure of personal information

11.1 The record-keeper shall not disclose personal information to a person, body or agency unless certain exceptions apply. Relevant exceptions include:

- the individual is reasonably likely to have been aware, or made aware under IPP2, that information of that kind is usually passed to that person, body or agency;
- the individual concerned has consented to the disclosure;
- the disclosure is required or authorised by or under law; or
- the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

Analysis of compliance with IPP11

11.2 It is not intended that DHS will disclose any personal information in Release 1 and accordingly Release 1 does not raise risk of non-compliance with IPP11.

11.3 However, DHS should not disclose any personal information unless it first obtains legal advice that the disclosure is authorised under IPP11 or APP6 from 12 March 2014.

Department of Human Services introduction of myGov (Release 1)

Privacy Impact Assessment

Attachment B – Privacy Statement

8 May 2013

HWL EBSWORTH
LAWYERS

Attachment B – Privacy Statement

Privacy Statement

This statement applies to personal information provided to the myGov website. The website is managed by the Department of Human Services on behalf of the Australian Government. The department is required to comply with the *Privacy Act 1988*.

The department collects personal information that you give it through myGov, such as your email address. We will use your personal information to establish and administer your myGov account.

If you wish to link your myGov account to a Member Service's online account you may select which of the following two actions is taken by the department (unless the Member Service has a specific requirement as to which one applies):

- the department will transfer you to that Member Service's website landing page to undertake an authentication process to ensure that your myGov account is linked to the correct record.
- the department will collect your personal information from the Member Service and use it to conduct the authentication and account linking process. The department will not hold this personal information after it has performed the authentication and account linking process. The questions you are asked and your answers will be held by the Member Service to whose account you are seeking to link.

We will only use your personal information, or share it with another organisation or government agency, for a different purpose if you consent to that other purpose, or that other purpose is required or authorised by law.

The department also collects information about how users use the myGov website (such as browsing and searching patterns). We collect this information to assist us to improve our website service. In undertaking this analysis, we will not identify users, or their use of the website, unless authorised by law. For example, we might inspect the audit logs of a user if the inspection is reasonably necessary for the enforcement of the criminal law.

If you wish to access your personal information, or discuss privacy issues associated with myGov, please call Customer Relations on **1800 050 004** or the TTY phone on **1800 000 567**.

For more information about our privacy practices, see our full privacy statement **[insert link to myGov full Privacy Statement]**

Full privacy statement

The myGov website is managed by the Commonwealth Department of Human Services on behalf of the Australian Government. The myGov website now hosts user accounts that were previously hosted on the australia.gov.au website.

This Privacy Statement applies to the myGov website only. Separate privacy statements apply to the Department of Human Services' Centrelink, Medicare and Child Support programs and the other Australian Government agencies to whose websites you may link from the myGov website. These other Australian Government agencies are known as Member Services.

This Privacy Statement explains how the department collects, through the *myGov* website, personal information from you and:

- how the department will use and disclose that information;
- how the department will store and secure that information; and
- how you can access and alter your personal information.

Collections

If you held an australia.gov.au account that account is now managed through this website.

The australia.gov.au account information held by the department at the time of the transition from australia.gov.au to myGov does not contain any personal information. This is because all australia.gov.au account holders are anonymous as account user 'names' consist of a combination of numbers and letters that do not identify the individual. The accounts hold only a limited amount of information which the department cannot use to identify the individual account holder.

Existing australia.gov.au account holders who wish to use their newly named myGov account, and new users will both be required to provide to the department, through myGov:

- an email address, and may also provide a mobile phone number, for account creation and to implement the user name recovery service feature of myGov; and
- a password and at least three secret questions and answers.

Upon receipt by the department of the above information, the user will automatically be provided with a user ID for their myGov account.

The department will also maintain audit logs of activity in relation to your account such as last login, attempted logins and password changes. You can see much of this in your account history.

There are two ways in which you can link to a Member Service - Options 1 and 2 described below. A Member Service may require that you use a particular Option, but in the absence of such a requirement you may choose which Option you follow.

Option 1

If you wish to link your myGov account to a Member Service's online account, the department will transfer you to that Member Service's website landing page to undertake an authentication process to ensure that your myGov account is linked to the correct record.

Option 2

The department will collect your personal information from the Member Service and use it to conduct the authentication and account linking process. The department will not hold this personal information after it has performed the authentication and account linking process. The questions you are asked and your answers will be held by the Member Service to whose account you are seeking to link.

You may opt out of any further use of myGov in which case you can contact Member Services directly.

Uses and Disclosures

We will use your personal information for the purposes for which you gave it to us. Those purposes include establishing, maintaining and performing administration in relation to your myGov account and the links between that account and the Member Services.

We will only share your personal information with other organisations or government agencies if it:

- is necessary to provide you with a service that you have requested (including enabling us to link your accounts); or
- is necessary to complete an activity that you have chosen to undertake.

We will only use your personal information, or disclose it to another organisation or government agency, for another purpose if you consent or if that other purpose:

- is required or authorised by law;
- will prevent or lessen a serious and imminent threat to somebody's health; or
- is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of public revenue.

Cookies

We analyse non-identifiable website traffic data to improve our services. Cookies are pieces of information that a website can transfer to an individual's computer. We do not use persistent cookies. We only use session-based cookies for the single sign-on service and to gather anonymous website usage data to help us improve the structure and functionality of myGov. You can change your web browser settings to reject cookies or to prompt you each time a website wishes to add a cookie to your browser. Some functionality on the website may be affected by this.

We will not attempt to identify users or their browsing activities. However, there are some circumstances when we may need to disclose information that may be used to identify users to law enforcement authorities, namely if the disclosure:

- is required or authorised by law;
- will prevent or lessen a serious and imminent threat to somebody's health; or
- is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of public revenue.

Data security

We take steps to protect the personal information we hold against loss, unauthorised access, use, modification or disclosure and against other misuse. These steps include storing electronic files in secure facilities, encryption of data, regular backups of data we hold, audit and logging mechanisms and physical access restrictions.

When no longer required, personal information is destroyed in a secure manner.

Access to and correction of your personal information

You may gain access to personal information about you that we hold and more specifically any personal information collected as a result of our management of myGov unless the department is required or authorised by law to refuse to allow you to access the record.

You can have us correct any errors or delete the information we have about you unless there is a sound reason under any law not to make the change. Information from you can be added to your record if we decide not to change it.

To protect your privacy and the privacy of others, we may have to gain evidence of your identity before we can give you access to information about you or change it.

Important information

The department is required to ensure this website complies with the Information Privacy Principles in section 14 of the Privacy Act 1988.

We also follow the *Guidelines for federal and ACT government websites* issued by the Office of the Australian Information Commissioner.

How to contact us

If you wish to access your personal information, or if you are concerned about how myGov has collected or managed your personal information, please call Customer Relations on **1800 050 004** or the **TTY phone** on **1800 000 567**.

Obligations for Australian Government agencies

With respect to the collection, use, storage and disclosure of personal information, we are bound by the *Information Privacy Principles in section 14 of the Privacy Act 1988*. We also follow the *Guidelines for federal and ACT government websites* issued by the Office of the Australian Information Commissioner. The Office of the Australian Information Commissioner has issued a number of guidelines, including the *Guidelines to the information privacy principles*, which apply to all Australian Government departments and agencies.

For more information about privacy obligations for Australian Government agencies please visit:

Office of the Australian Information Commissioner

Your privacy rights faqs

Privacy Act 1988[1]

Information privacy principles under the Privacy Act 1988

Guidelines for federal and ACT government websites

[1] http://www.comlaw.gov.au/Details/C2013C00125

Multi-layered privacy notices

The multi-layered privacy notices format used by myGov takes up the recommendation of the Privacy Commissioner in Recommendations 19 and 20 of 'Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988'. These recommendations support the development of short form privacy notices.

Multi-layered privacy notices have also been endorsed by Data Protection and Privacy Commissioners in 2003, further developed in the Berlin Memorandum, and endorsed in Opinion WP 100 by the Article 29 Committee of European Data Protection and Privacy Commissioners.

Multi-layered privacy notices are based on the work of the Centre for Information Policy Leadership.

For more information about the multi-layered privacy notice format used in my.gov.au please visit:

- Getting in on the Act: the review of the private sector provisions of the Privacy Act 1988
- Getting in on the Act - recommendations: control over personal information
- Privacy notice resolution resources (International Conference of Data Protection & Privacy Commissioners (25th : Sydney, 2003))
- Berlin privacy notices memorandum
- Data protection (European Commission)
- Centre for Information Policy Leadership