PRIVACY IMPACT ASSESSMENT REPORT

DSS DATA EXCHANGE

^22 September 2015^

To: Department of Social Services

CONTENTS

PRIVACY IMPACT ASSESSMENT REPORT

DSS DATA EXCHANGE

1. EXECUTIVE SUMMARY

Purpose of this PIA

1.1. The purpose of this Privacy Impact Assessment (PIA) is to identify the possible impacts that the DSS Data Exchange might have on the privacy of individuals. In relation to possible negative impacts, this PIA makes recommendations for managing, minimising or eliminating those impacts.

1.2. This assessment of possible privacy impacts involves an assessment of whether there is any risk that the DSS Data Exchange is being operated in a way that does not comply with the *Privacy Act 1988* (Cth) (Privacy Act) - in particular, the Australian Privacy Principles (APPs) as set in Schedule 1 to that Act. In relation to assessing any risk of non-compliance with the APPs, APP 1.2 requires the Department of Social Services (the Department) to take reasonable steps to implement procedures relating to the Department's operation of the DSS Data Exchange that will:

- ensure that the Department complies with the APPs; and
- enable the Department to deal with inquiries or complaints from individuals about the Department's compliance with the APPs.

1.3. This PIA is a key procedural means for assessing any risk that the Department is not complying with the APPs in operating the DSS Data Exchange.

1.4. An assessment of the impacts that the DSS Data Exchange might have on the privacy on individuals should also assess broader impacts – including, in particular, whether the DSS Data Exchange complies with community privacy expectations. The ongoing feedback that the Department receives from community stakeholders – in particular, service providers and clients of service providers – is obviously highly relevant to an assessment of these broader impacts.

A broad description of the data that flows through the DSS Data Exchange: 'Data requirements' that are involved in grant programmes reporting, and additional data sources

1.5. The DSS Data Exchange is an Information Technology (IT) system that facilitates the Department's new approach to grant programmes reporting.

Data requirements that are involved in grant programmes reporting

1.6. In July 2014, the Department published 'The DSS Data Exchange Framework: A new approach for streamlined programme performance reporting' (the DSS Data Exchange Framework document). That document is intended to be used as the key reference document for the new approach to programme performance reporting (see section 1.3 of the DSS Data Exchange Framework).

1.7. Section 1.2 of the DSS Data Exchange Framework document provides an introduction to the 'DSS Data Exchange Framework'. According to the introduction, data requirements are divided into 2 parts: 'a small set of mandatory *priority requirements* that all service providers report, and a voluntary extended data set that providers can choose to share with the Department in exchange for relevant and meaningful reports, known as the *partnership approach*.' The mandatory priority requirements, together with the partnership approach, 'build the evidence base regarding the effectiveness of DSS programmes and service delivery approaches.' The document mentions that '[p]articipation in the *partnership approach* is entirely voluntary and there will be no negative consequences if a service provider chooses not to provide the extended data set.'

1.8. Section 1.2 of the DSS Data Exchange Framework document mentions that the DSS Data Exchange Framework 'also covers two additional sources of outcome data that will be collated by DSS and shared with service providers who participate in the *partnership approach*', being 'population data sourced from other government data sets and outcomes data from follow-up client surveys.'

Additional data sources

Additional outcomes data to be collected through follow-up client surveys

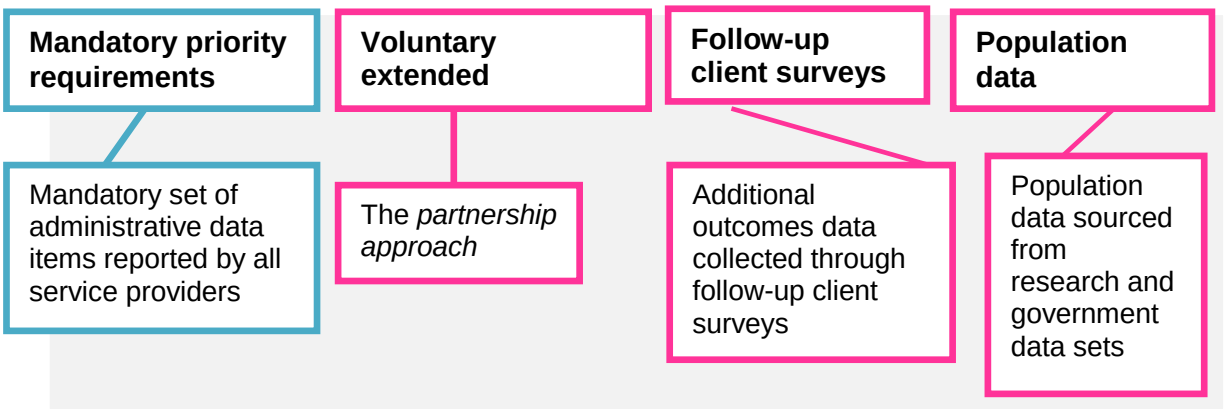
1.9. According to section 7 of the DSS Data Exchange Framework document, arrangements for the collection of additional follow-up client survey data sets will be established through sector consultations, and the conduct of surveys 'will require clear purpose and full ethics approval.' The Department intends to collect programme performance data through such surveys, which would complement data of this kind that is collected through grant programmes reporting.

Population data sourced from research and government data sets

1.10. Population data sets are addressed at section 8 of the DSS Data Exchange Framework document. Population data sets that are based on research are collated by the Department and draw on established research collections such as those of the Australian Bureau of Statistics and the Australian Institute of Health and Welfare.

1.11. Additional sources of population data are to be generated by the Department through matching clients of service providers across DSS programme activities and with government data sets, with this matching to occur on a 'de-identified basis' through the use of a statistical linkage key: see, for example, section 4.1 of the DSS Data Exchange Framework document.

1.12. The data requirements sourced from service providers, and the additional data sources, are depicted in a diagram in section 1.3 of the DSS Data Exchange Framework document. That diagram is reproduced below:



1.13. Section 2 of the PIA - 'PIA Methodology' – summarises how this PIA was conducted.

1.14. Section 3 of this PIA - 'DSS Data Exchange Description' - provides a description of:

- the arrangements in place between the Department and service providers for grants programme reporting, and how those requirements are facilitated by the DSS Data Exchange; and
- the arrangements that have been put in place between the Department and service providers for the anticipated collection of additional data through follow-up client surveys.

Table of recommendations

1.15. Section 4 of this PIA - 'Analysis' - makes recommendations for managing, minimising and eliminating the possible negative impacts that the Department's operation of the DSS Data Exchange might have on the privacy of individuals. The table below sets out the recommendations that have been made and, for each recommendation, gives a page reference to the relevant part of section 4.

NUMBER	RECOMMENDATION	PAGE REFERENCE
1	Review and update the Department's general APP privacy policy now to ensure that it reflects the Department's specific practices for managing personal information in relation to its operation of the DSS Data Exchange. Additionally, regularly review that policy, and update it as necessary, to ensure that it reflects any changes to the Department's specific information handling practices relating to the DSS Data Exchange.	11
2	Take appropriate steps to ensure that, when accessing the database in which client-level unit records are stored, database administrators understand why they need to comply with relevant Departmental privacy and security procedures, and how they are to comply with these procedures.	16
3	To eliminate the risk that the Department is presently operating the DSS Data Exchange in a way that does not	18

NUMBER	RECOMMENDATION	PAGE REFERENCE
	comply with APPs 3.1 and 3.3, decide, as a matter of priority, whether the client management system functionality of the Exchange will be made available to service providers who undertake programme reporting by way of system to system transfers or bulk uploads.	
4	Confirm the need for service providers to store client contact details to facilitate follow-up client surveys.	19
5	Enhance present arrangements with service providers using the web-based portal as a client management system to ensure that the Department is fully complying with APPs 3.3(a)(i) and 3.6 in collecting a client's personal information from those service providers.	20
6	Revise the 'DSS standard notification' to ensure that the Department is appropriately complying with APP 5 in collecting a client's personal information through service providers who are using the web-based portal as a client management system.	23
7	Regularly assess the risk that the Department might be disclosing 'new' personal information about clients to service providers in the reporting context.	25

1.16. Section 5 of this PIA - 'Response to Recommendations' - discusses the Department's response to each recommendation. The details of the Department's response to each recommendation are set out in the Table in **Appendix 7**.

2. PIA METHODOLOGY

Key documentation

2.1. The conduct of this PIA was based on considering the following 2 key documents about the DSS Data Exchange:

1) the DSS Data Exchange Framework document, which is the key reference document for the policy underpinning the DSS Data Exchange; and

2) 'The *DSS Data Exchange* Protocols' (the DSS Data Exchange Protocols document), which is a practical support manual for service providers.

2.2. As mentioned elsewhere in this PIA, both of these documents have been published by the Department.

Information from the Department

2.3. In conducting this PIA, further information from the Department was sought and received by us in relation to various matters addressed in the 2 key documents mentioned above, as well as in relation to various other matters concerning the Department's operation of the DSS Data Exchange.

Map of the process for the reporting of client-level data by service providers through the DSS Data Exchange

2.4. Undertaking this PIA involved the Department mapping in detail the process for the reporting of client-level data by service providers through the DSS Data Exchange: see **Appendices 2 and 3**, which are considered below in Section 4.

3. DSS DATA EXCHANGE DESCRIPTION

Arrangements in place between the Department and service providers for grants programme reporting, and how those requirements are facilitated by the DSS Data Exchange

Reporting requirements for grants programme reporting are specified in grants agreements

3.1. If the DSS Data Exchange applies to a grant programme, the reporting requirements for the programme, including how those requirements are facilitated by the DSS Data Exchange, are specified in a grant agreement between the Commonwealth (as represented by the Department) and the service provider.

3.2. Grant agreements are in the form of the 'DSS Streamlined Grant Agreement' or 'DSS Comprehensive Grant Agreement'. We have been informed by the Department that the 'DSS Streamlined Grant Agreement' is presently being used for somewhere around 90% of service providers.

Typical reporting requirements for service providers

3.3. We have been provided with an example of the DSS Streamlined Grant Agreement. The reporting requirements for the service provider that are specified in this example are described immediately below.

3.4. The relevant service provider is required to:

- report certain data 'in accordance with the DSS Data Exchange Protocols document'; and
- report that data using an 'approved mechanism', being system to system transfers, bulk uploads or the web-based portal; and
- finalise data reporting for each reporting period within 30 days of the reporting period ceasing.

3.5. The example 'DSS Streamlined Grant Agreement' requires the grant service provider to undertake reporting in two, six-month reporting periods over a year – one reporting period is from 1 January to 30 June of a relevant year, and the other reporting period is from 1 July to 31 December of a relevant year.

3.6. This PIA proceeds on the basis that the reporting requirements described above are the same for all grant programmes to which the DSS Data Exchange applies.

Approved reporting mechanisms

3.7. The DSS Data Exchange allows a service provider to undertake programme reporting by way of system to system transfers, bulk uploads or the web-based portal.

System to system transfers

3.8. For system to system transfers, the Department has published the 'DSS Data Exchange System Web Services Technical Specifications' (Current Version Number: 1.3; Revision Date: 15 October 2015,). Service providers using system to system transfers undertake programme reporting with a third party software application that uses the 'DSS Data Exchange System Web Services interface'. The 'DSS Data Exchange System Web Services Technical Specifications' provide technical details for service providers about this process – specifically, the technical specifications for developing this web services capability.

Bulk uploads

3.9. For bulk uploads, the Department has published the 'DSS Data Exchange System Bulk File Upload Technical Specifications' (Version Number: 1.1; Revision Date: 28 November 2014). Service providers using bulk uploads undertake programme reporting by uploading an XML file to the DSS Data Exchange. The 'DSS Data Exchange System Bulk File Upload Technical Specifications' provides technical details for this process – specifically, the technical specifications for developing this bulk file upload capability.

Web portal

3.10. The DSS Data Exchange includes a web-based portal that can be utilised by service providers to undertake programme reporting. Service providers using the portal undertake programme reporting by completing the web-based forms that are available in that portal. The Department has published 'Task Cards' and 'E-Learning Modules' to assist service providers in understanding the functions of the portal. The web-based portal can also be used as a client management system by the service provider for its own purposes.

3.11. This PIA does not include an assessment of whether the *technological* operation of the system to system transfer, bulk upload, or web-based portal programme reporting processes involves any possible impacts on the privacy of individuals, that is, security risks to the personal information of individuals. Further, this PIA does not include an assessment of whether the *technological* operation of the web-based portal, insofar as it is used as a case management system, gives rise to any possible impacts on the privacy of individuals. We think that an assessment of these matters, if appropriate, would be appropriately conducted through other means – for example, through an information security risk assessment. We mention that the Office of the Australian Information Commissioner's (OAIC) *Guide to securing personal information*, which is accessible on the website of the OAIC, discusses various means by which security risks to personal information can be appropriately assessed.

Arrangements that have been put in place between the Department and service providers for the anticipated collection of additional data through follow-up client surveys

3.12. The arrangements that have been put in place between the Department and service providers for the anticipated collection of additional data through follow-up client surveys are described at sections 4.4 and 5.4 of the DSS Data Exchange Protocols document. They are as follows:

- service providers are required to ask a client if he or she is willing to participate in client research, and are required to report the client's answer as one of the mandatory priority requirements; and
- 'in order to contact a client at a later date service providers are asked to store client contact details such as phone numbers or email addresses separately to the *DSS Data Exchange*'. Such 'information may be used to facilitate contact with the client for an ethics approved research activity in the future'.

Map of information flows

3.13. As mentioned above, undertaking this PIA involved the Department mapping in detail the process for the reporting of client-level data by service providers through the DSS Data Exchange: see **Appendices 2 and 3**, which are considered below in Section 4.

4. ANALYSIS

Assessment of any risk of non-compliance of DSS Data Exchange with APPs

4.1. This section, which is structured by reference to each relevant APP:

- assesses whether there is any risk that the Department is not complying with the APP in operating the DSS Data Exchange; and
- where such a risk might exist, sets out recommendations for managing, minimising or eliminating that risk.

Australian Privacy Principles guidelines

4.2. The Australian Information Commissioner (AIC) has made and published the Australian Privacy Principles guidelines (APP guidelines) under section 28 of the Privacy Act. Whilst the APP guidelines are not legally binding, they outline the AIC's interpretation of the APPs, provide examples of how the APPs may apply in particular circumstances, and outline good privacy practice to supplement minimum compliance with the mandatory requirements in the APPs. This section of the PIA refers to the APP guidelines as appropriate.

APPs that are not relevant to an analysis of the DSS Data Exchange

4.3. We have concluded that the following APPs are not relevant to an analysis of the DSS Data Exchange:

- APP 2, which together with APP 1, relates to the consideration of personal information privacy; and
- APP 4, which is one of a number of APPs that deal with the collection of personal information; and
- APPs 7, 8 and 9, which, in addition to APP 6, relate to dealing with personal information.

4.4. The considerations that were taken into account in relation to APPs 2, 4, 7, 8 and 9 are set out below.

APP 2 – anonymity and pseudonymity

4.5. APP 2 provides that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with the Department in relation to a particular matter (APP 2.1). APP 2.1 does not apply if an exception in APP 2.2 operates in relation to the matter in question.

4.6. We think that it is reasonable to proceed on the basis that the Department is not required to comply with APP 2 in relation to its present operation of the DSS Data Exchange. This is because, in operating the Exchange, the Department is not dealing with individuals in relation to any particular matters. Rather, in this context, it is service providers who are dealing with individuals in relation to particular matters – by providing Department-funded services to clients.

APP 4 – dealing with unsolicited personal information

4.7. APP 4 relates to dealing with unsolicited personal information, and sets out what the Department must do if it has received such information. According to the definition of 'solicits' in s 6(1) of the Privacy Act, the Department solicits personal information if it 'requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included.' Section 6(1) provides that an entity is an agency, organisation or small business operator. The term 'agency' is defined in s 6(1), and the terms 'organisation' and 'small business operator' are defined in sections 6C and 6D, respectively.

4.8. For the purposes of the definition of 'solicits' in s 6(1) of the Privacy Act, having regard to grant agreements that are in place between the Commonwealth and service providers, it can be said that the data requirements sourced from service providers (that is, the mandatory priority requirements and voluntary extended requirements) are 'requested' by the Department from the service providers. This PIA proceeds on the basis that service providers are all 'organisations' as defined in s 6C.

4.9. We therefore proceed on the basis that any personal information included in the data requirements sourced from service providers will not be unsolicited personal information for the purposes of APP 4. On that basis, we conclude that APP 4 does not apply to the operation of the DSS Data Exchange.

APP 7 – direct marketing

4.10. If an organisation holds personal information about an individual, APP 7 regulates the organisation's use or disclosure of that information for the purposes of direct marketing. 'Direct marketing involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services': see para 7.9 of the APP guidelines.

4.11. The Department is an 'agency' (s 6C of the Privacy Act), rather than an 'organisation' (s 6D). However, s 7A of the Privacy Act provides for acts or practices of certain agencies to be treated as the acts or practices of an organisation.

4.12. As far as we are aware, in operating the DSS Data Exchange, the Department does not use or disclose personal information it holds about an individual for the purposes of direct marketing. Further, having considered the terms of s 7A, we have established that s 7A does not deem any acts or practices of *the Department* to be the acts or practices of an organisation. On this basis, we conclude that APP 7 has no legal application to the Department's operation of the DSS Data Exchange.

APP 8 – cross-border disclosure of personal information

4.13. The Department is required to comply with APP 8 if it discloses personal information about an individual to a person (the overseas recipient) who is not in Australia or an external Territory, and where the overseas recipient is not the Department or the individual about whom the personal information is concerned.

4.14. In the course of operating the DSS Data Exchange, the Department discloses personal information to a service provider (being the personal information of a client of a provider in circumstances where the service provider is using the web-based portal as a client management system for its own purposes). This PIA proceeds on the basis that:

- all service providers are in Australia; and
- the Department does not intend to send or store personal information overseas.

4.15. On this basis, we conclude that the Department is not required to comply with APP 8 in its operation of the DSS Data Exchange.

APP 9 – adoption, use or disclosure of government related identifiers

4.16. APP 9 regulates the adoption of government related identifiers by organisations. It also regulates the use or disclosure of government related identifiers by organisations. As discussed above in relation to APP 7, although the Department is an 'agency' (s 6C of the Privacy Act), rather than an 'organisation' (s 6D), s 7A of the Privacy Act provides for acts or practices of certain agencies to be treated as acts or practices of an organisation. However, the agencies covered by s 7A do not include the Department. On this basis, we conclude that APP 9 has no legal application to the Department's operation of the DSS Data Exchange.

APPs that are relevant to an analysis of the DSS Data Exchange

4.17. The APPs that are relevant to an analysis of the DSS Data Exchange are as follows:

- APP 1, which relates to the consideration of personal information privacy; and
- APPs 3 and 5, which deal with the collection of personal information; and
- APP 6, which relates to dealing with personal information; and
- APPs 10 and 11, which deal with the integrity of personal information; and
- APPs 12 and 13, which deal with access to, and correction of, personal information.

4.18. We address each of the above APPs below.

APP 1 - open and transparent management of personal information

4.19. The object of APP 1, which relates to the consideration of personal information privacy, is to ensure that the Department manages personal information in an open and transparent way (APP 1.1).

4.20. APP 1 imposes the following obligations upon the Department:

- to take reasonable steps to implement practices, procedures and systems that will ensure the Department complies with the APPs, and is able to deal with related inquiries and complaints (APP 1.2).
- to have a clearly expressed and up-to-date APP privacy policy about how the Department manages personal information (APPs 1.3 and 1.4).
- to take reasonable steps to make its APP privacy policy available free of charge in an appropriate form (APP 1.5) and, upon request, in a particular form (APP 1.6).

4.21. As discussed above, this PIA is a key procedural means for assessing any risk that the DSS Data Exchange is being operated in a way that does not comply with the APPs (APP 1.2). The Department's obligations under APPs 1.5 and 1.6 are relevant to all of the Department's functions or activities that involve the management of personal information, and are not given any particular consideration in this PIA.

4.22. The Department's obligations under APPs 1.3 and 1.4 are particularly relevant to an analysis of the Department's operation of the DSS Data Exchange, and are considered below.

APPs 1.3 and 1.4: APP Privacy Policy

4.23. As mentioned above, the Department must have a clearly expressed and up-to-date policy - an APP privacy policy - about the management of personal information by the Department (APP 1.3). According to APP 1.4, the APP privacy policy of the Department must include the following information:

- the kinds of personal information that the Department collects and holds;
- how the Department collects and holds personal information;

- the purposes for which the Department collects, holds, uses and discloses personal information;
- how an individual may access personal information about the individual that is held by the Department and seek the correction of such information;
- how an individual may complain about a breach of the APPs, and how the Department will deal with such a complaint;
- whether the Department is likely to disclose personal information to overseas recipients; and
- if the Department is likely to disclose personal information to overseas recipients – the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Analysis

4.24. The Department's APP privacy policy (**Appendix 1**) is available on the Department's website, and was last updated on 10 March 2015. It includes all of the information that is required to be included under APP 1.4. The Department's APP privacy policy is a general policy that is intended to address all of the various functions and activities of the Department that involve the management of personal information. The Department's functions and activities include its operation of the DSS Data Exchange.

4.25. Paragraph 1.9 of the APP guidelines state that an APP entity should regularly review and update its APP privacy policy to ensure that it reflects the entity's information handling practices. In keeping with this guidance, the Department should review and update its general APP privacy policy now to ensure that it reflects the Department's specific practices for managing personal information in relation to its operation of the DSS Data Exchange. The Department should also regularly review that policy, and update it as necessary, to ensure that it reflects any changes to the Department's specific information handling practices relating to the DSS Data Exchange.

Recommendation 1: Review and update the Department's general APP privacy policy now to ensure that it reflects the Department's specific practices for managing personal information in relation to its operation of the DSS Data Exchange. Additionally, regularly review that policy, and update it as necessary, to ensure that it reflects any changes to the Department's specific information handling practices relating to the DSS Data Exchange.

APP 3 - collection of solicited personal information

4.26. APP 3 applies to the collection of personal information that is solicited by the Department (APP 3.7).

Personal information other than sensitive information

4.27. The Department must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, the Department's operation of the DSS Data Exchange (APP 3.1)

Sensitive information

4.28. The Department must not collect sensitive information about an individual unless the individual consents to the collection of the information and the information is reasonably necessary for, or directly related to, the Department's operation of the DSS Data Exchange (APP 3.3(a)(i)).

Means of collection

4.29. The Department must collect personal information only by lawful and fair means (APP 3.5).

4.30. According to APP 3.6, the Department must collect personal information about an individual only from the individual unless:

- the individual consents to the collection of the information from someone other than the individual; or
- the Department is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or
- it is unreasonable or impracticable to do so.

Analysis

The Department collects solicited information from service providers

4.31. According to the definition of 'solicits' in section 6(1) of the Privacy Act, the Department solicits personal information if it 'requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included.' Section 6(1) provides that an entity is an agency, organisation or small business operator. The term 'agency' is defined in section 6(1), and the terms 'organisation' and 'small business operator' are defined in sections 6C and 6D, respectively.

4.32. For the purposes of the definition of 'solicits' in section 6(1) of the Privacy Act, having regard to grant agreements that are in place between the Commonwealth and service providers, it can be said that the data requirements sourced from service providers (that is, the mandatory priority requirements and voluntary extended requirements) are 'requested' by the Department from the service providers. Further, this PIA proceeds on the basis that service providers are all 'organisations' as defined in section 6C and are, therefore, 'entities'.

4.33. We therefore proceed on the basis that any personal information included in the data requirements sourced from service providers will be 'solicited' personal information for the purposes of APP 3.

4.34. We also proceed on the basis that any personal information so provided will be collected by the Department when it is *stored* in the DSS Data Exchange, which is an IT system. According to section 6(1) of the Privacy Act, the Department 'collects' personal information only if it collects the personal information for inclusion in a

record (or generally available publication). We think that personal information *stored* in the DSS Data Exchange – an IT system – will be stored in a 'record' for the purposes of the Privacy Act (and see the definition of 'record' in section 6(1)).

To what extent is the solicited information being collected by the Department from service providers 'personal information'?

4.35. A key matter for determination is the extent to which the solicited information being collected by the Department from service providers is 'personal information'.

4.36. As discussed above, reporting requirements for grant programmes to which the DSS Data Exchange applies require service providers to report in accordance with the DSS Data Exchange Protocols document. The DSS Data Exchange Protocols document has been published by the Department on its website. The current version was published on 10 March 2015.

4.37. According to the DSS Data Exchange Protocols document, grant reporting requirements under the DSS Data Exchange require service providers to report client-level data.

4.38. Where, however, 'the collection of client level data is not practical or appropriate, for instance due to an activity involving a large group of people or a whole community, aggregate reporting is accommodated': see section 2.1 of the DSS Data Exchange Protocols document. Aggregate reporting is also described at section 5.2.3. It is clear that the information that the Department solicits from service providers through aggregate reporting is not 'personal information'.

4.39. Client-level data is reported to the Department in the form of client-level unit records (see section 3 of the DSS Data Exchange Framework document), and the Department has confirmed that the reported data is also collected (or stored) by the Department in that form. The key matter to be determined is, therefore, the circumstances in which a client-level unit record is 'personal information'. This matter is considered below.

4.40. Data items that make up the mandatory priority requirements are recorded in the 'standard client-level unit record'. These data items are summarised in Table A1.1 of the DSS Data Exchange Framework document, and list of possible data values for each data item is provided on page 44 of the DSS Data Exchange Protocols document under the heading 'Client record – mandatory priority requirements'.

4.41. Data items that make up the voluntary extended requirements are also recorded in the 'standard client-level unit record' which, when it includes these items, is known as the 'extended client-level unit record'. The data items that make up the voluntary extended requirements are summarised in Table A2.1 of the DSS Data Exchange Framework document, and list of possible data values for each data item is provided on pages 46 to 47 of the DSS Data Exchange Protocols document under the heading 'The voluntary extended data set – the partnership approach'.

4.42. Undertaking this PIA involved the Department mapping in detail the process for the reporting of client-level data. The Table at **Appendix 2** describes the reporting process where the reporting of the client's first name and last name is involved, and

the Table at **Appendix 3** describes the reporting process where the reporting of the client's pseudonym is involved.

4.43. In each Table, the column headed 'Information stored by DSS' sets out the information that is stored, and therefore, collected by the Department in the DSS Data Exchange.

4.44. Considering first the Table at **Appendix 2** (where the reporting of the client's first and last name is involved), this PIA proceeds on the basis that the Department collects personal information in scenarios 1A, 1B, 3 and 5. This is because the data sets that are stored in client-level unit records in the DSS Data Exchange in these scenarios include the relevant client's first name and last name, and can also include the client's full residential address.

4.45. In scenarios 2, 6 and 7, it is not obvious that the Department is collecting personal information. This is because the data sets that are stored in client-level unit records in the DSS Data Exchange in these scenarios do not include the client's first name, last name and full residential address. In each of these scenarios, however, the data set that is stored in a client-level unit record includes a statistical linkage key. The DSS Data Exchange uses the Australian Institute of Health and Welfare Statistical Linkage Key 58. In this PIA, this Statistical Linkage Key is referred to as the 'SLK'.

4.46. The nature of the SLK is explained at para 5.2.2 of the DSS Data Exchange Protocols document, as follows:

> Technically, the SLK is a code consisting of the second, third and fifth characters of a person's family name, the second and third letters of the person's given name, the day, month and year when the person was born and the sex of the person.
>
> For example John Smith, a male born on 14th February 1971 has an SLK of: MIHOH140219711.

4.47. Further information about the way in which the SLK is coded is available on the website of the Australian Institute of Health and Welfare (on a webpage entitled 'Statistical linkage key 581 cluster').

4.48. In the Privacy Act, 'personal information' includes 'information or an opinion' 'about … an individual who is reasonably identifiable' (see section 6(1)). This definition was updated in 2012 by the *Privacy Protection (Enhancing Privacy Protection) Act 2012*, and extrinsic material for the associated Bill included the following explanation of 'reasonably identifiable':

> The new definition will refer to an individual who is, 'reasonably identifiable'. Whether an individual can be identified or is reasonably identifiable depends on context and circumstances. While it may be technically possible for an agency or organisation to identify individuals from information it holds, for example, by linking the information with other information held by it, or another entity, it may be that it is not practically possible. For example, logistics or legislation may prevent such linkage. In these circumstances, individuals are not 'reasonably identifiable'. Whether an individual is reasonably identifiable from certain information requires a consideration of the cost, difficulty, practicality and likelihood that the information will be linked in such a way as to identify him or her.

> … Guidance issued by the OAIC would play an important role in assisting organisations, agencies and individuals to understand the application of the new definition, especially given the contextual nature of the definition.

4.49. According to this extrinsic material, determining whether an individual is reasonably identifiable from particular information or a particular opinion is not limited to simply considering the particular information or particular opinion. The APP guidelines (paras B.91 to B.94) provide that a person may be reasonably identifiable from particular information having regard certain considerations, which include:

- who will have access to the information
- other information either held by or available to the APP entity that holds the information
- whether it is possible for the entity that holds the information to identify the individual, using available resources (including other information available to that entity).

4.50. The APP guidelines also state, by reference to the above mentioned extrinsic material, that:

> [w]hether a person is 'reasonably identifiable' is an objective test that has practical regard to the context in which the issue arises. Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood of its occurring, the information would not generally be regarded as 'personal information'.

4.51. The Department has informed us that its security arrangements, as set out in the Department's ICT Security Policy, operate so that employees of the Department cannot access the database in which client-level unit records are stored, with the exception of a highly restricted number of employees who perform database administration duties. The Department's Information Management and Technology Group has confirmed that, to perform their duties, database administrators are required to hold security clearances at a level that reflects government requirements for access. The Department has also informed us that access by database administrators is conditional upon them having signed a confidentiality agreement, administrators are required to follow Departmental privacy and security procedures that prevent 'browsing' and sharing of information, and that the activities undertaken by administrators are monitored.

4.52. In relation to each of scenarios 2, 6 and 7, it seems that it might be technically possible to identify the relevant individual to whom the data set in the client-level unit record relates if a database administrator:

- held, or was able to obtain, a *comprehensive* list of the first names, last names, and dates of birth of individuals residing in the relevant suburb or post code; and
- could cross-reference the information in that list with the information in the client-level unit record to establish the identity of the relevant individual.

4.53. From a practical perspective, it seems that it would not be *technically possible* for a database administrator to identify relevant individuals. Having regard to the very nature of the lists described above, it seems that they would not be held by, or available to, the Department and, even if such lists were held or available, the cross-referencing activity that would be required would not necessarily lead to a certain identification.

4.54. In any case, in relation to each of scenarios 2, 6 and 7, the existence of a technical possibility of identification does *not* mean that the relevant individual is reasonably identifiable. Whether the relevant individual is reasonably identifiable from the data-set in the client-level unit record *depends on the context and circumstances*. It is clear that the duties of database administrators are not concerned with seeking to identify the relevant individual. Further, the circumstances in which those duties are performed, including the existence of the Departmental privacy and security procedures with which administrators are to comply when accessing the relevant database, effectively prevent attempts at identification. We think that these factors lead to the conclusion that the data sets in these client-level unit records do not relate to individuals that are reasonably identifiable and are, therefore, not 'personal information'.

4.55. To minimise any risk that information in the database in which client-level unit records are stored is not being appropriately safeguarded, we recommend that the Department take appropriate steps to ensure that database administrators understand why they need to comply with relevant Departmental privacy and security procedures when accessing the database, and how they are to comply with these procedures.

Recommendation 2: Take appropriate steps to ensure that, when accessing the database in which client-level unit records are stored, database administrators understand why they need to comply with relevant Departmental privacy and security procedures, and how they are to comply with these procedures.

4.56. Turning to the Table at **Appendix 3** (where the reporting of the client's pseudonym is involved), it is useful to make the initial point that '[t]he use of a pseudonym does not necessarily mean that an individual cannot be identified': see para 2.8 of the APP guidelines.

4.57. In scenarios 1A, 1B, 3 and 5, the DSS Data Exchange enables the relevant client's pseudonym to be stored alongside other information that includes the mandatory priority requirements, and can also include the client's full residential address. As explained at para 5.1 of the DSS Data Exchange Data Protocols document, the mandatory priority requirements 'cover data items to uniquely reflect the client and their key demographic characteristics.' Against this background, and having regard to the fact that storage of a client's pseudonym might not necessarily mean that the client is anonymous, this PIA proceeds on the basis that the Department collects, or might collect, personal information in scenarios 1A, 1B, 3 and 5.

4.58. In scenarios 2, 6 and 7, it is not obvious that the Department is collecting personal information. This is because the data sets that are stored in client-level unit records

in the DSS Data Exchange in these scenarios do not include the client's pseudonym and full residential address. In these scenarios, however, the data set that is stored includes the SLK which, the Department has explained, has been coded using the client's pseudonym. The context and circumstances in which client-level unit records are accessed in scenarios 2, 6 and 7 is the same as the context in which those records are accessed where the reporting of the client's first name and last name is involved – that is, those records are accessed by the highly restricted number of employees who perform database administration duties in the circumstances described above. On that basis, this PIA concludes that the data sets in those client-level unit records do not relate to individuals that are reasonably identifiable and are, therefore, not 'personal information'.

The Department has documented its reasons for collecting the data sets that make-up client-level unit records (APPs 3.1 and 3.3(a)(i))

4.59. If a client-level unit record contains 'personal information', there is a reasonable prospect that it will also include 'sensitive information'. For example, the definition of 'sensitive information' in the Privacy Act includes information about an individual's racial or ethnic origin and one of the mandatory priority requirements that service providers report is a client's Indigenous status (see section 5.1.6 of the DSS Data Exchange Protocols document). By way of further example, the definition of 'sensitive information' also includes information about an individual's disability – in this respect, one of the mandatory priority requirements that is reported is information about a client's disability (see section 5.1.8 of the DSS Data Exchange Protocols document).

4.60. The effect of APPs 3.1 and 3.3 is that the Department must not collect personal information, including sensitive information, unless the information is reasonably necessary for, or directly related to, its operation of the DSS Data Exchange.

4.61. The Department has documented how its collection of the mandatory priority requirements and voluntary extended requirements relate to its operation of the DSS Data Exchange. For the mandatory priority requirements, these reasons are summarised in Table A1.1 of the DSS Data Exchange Framework document, and detailed in section 5 of the DSS Data Exchange Protocols document. For the voluntary extended requirements, these reasons are summarised in Table A2.1 of the DSS Data Exchange Framework document, and detailed in section 6 of the DSS Data Exchange Protocols document.

4.62. In scenario 1A of the Table at **Appendix 2**, and scenario 1A of the Table at **Appendix 3**, where the service provider is undertaking programme reporting by way of the web-based portal, the Department is storing the client's first name and last name, or pseudonym, together with the client's full residential address, in the portal because the Department is making that mechanism available to the provider to be used as a client management system for its own purposes.

4.63. In scenario 1B of the Table at **Appendix 2**, and scenario 1B of the Table at **Appendix 3**, where the service provider is undertaking programme reporting by way of the web-based portal, the Department is storing the client's first name and last

name, or pseudonym, in the portal because the Department is making that mechanism available to the provider to be used as a client management system for its own purposes.

4.64. In scenarios 3 and 5 of the Table at **Appendix 2**, and scenarios 3 and 5 of the Table at **Appendix 3**, where service providers are undertaking programme reporting by way of system to system transfers or bulk uploads, the Department has informed us that the operation of the DSS Data Exchange allows for storage of the client's first name and last name, or pseudonym, together with the client's full residential address, even though the Department has not made the client management system functionality of the Exchange available to these providers. Given these circumstances, it could be said that, in these scenarios, the Department presently has the capacity to collect personal information that is not reasonably necessary for, or directly related to, its operation of the DSS Data Exchange.

4.65. To eliminate the risk that the Department is presently operating this aspect of the DSS Data Exchange in a way that does not comply with APPs 3.1 and 3.3, the Department should give priority to deciding whether it will make the client management system functionality of the Exchange available to service providers who undertake programme reporting by way of system to system transfer or bulk uploads. If it is decided that this functionality will be made available to these service providers, the DSS Data Exchange Protocols document should be updated to reflect this decision. If it is decided that this functionality will not be made available to these service providers, the Department should alter the operational build of the DSS Data Exchange so that it does not allow for storage of a client's first name and last name, or pseudonym, together with the client's full residential address, where such information is reported by these providers.

Recommendation 3: To eliminate the risk that the Department is presently operating the DSS Data Exchange in a way that does not comply with APPs 3.1 and 3.3, decide, as a matter of priority, whether the client management system functionality of the Exchange will be made available to service providers who undertake programme reporting by way of system to system transfers or bulk uploads.

4.66. As discussed above, under the arrangements that have been put in place between the Department and service providers for the anticipated collection of additional data through follow-up client surveys, service providers are asked in the DSS Data Exchange Protocols document to store client contact details in the event that these details are required to undertake the surveys.

4.67. According to para 3.19 of the APP guidelines, '[f]actors relevant to determining whether a collection of personal information is reasonably necessary for a function or activity include' 'how the personal information will be used in undertaking a function or activity of the APP entity'. For example, 'in most circumstances collection on the basis that personal information could become necessary for a function or activity in the future' 'would not be necessary'. To eliminate any risk that personal information that is not 'reasonably necessary' to undertake follow-up client surveys is being collected on behalf of the Department by service providers, the Department should confirm that there is a need for service providers to store client contact

details to facilitate follow-up client surveys, and amend the DSS Data Exchange Protocols document accordingly (APP 3.1).

Recommendation 4: Confirm the need for service providers to store client contact details to facilitate follow-up client surveys.

Service providers report personal information with 'consent' (APPs 3.3(a)(i) and 3.6)

4.68. In circumstances where client-level data reported to the Department is, or might be, personal information, service providers report this data with 'consent': see scenarios 1A, 1B, 3 and 5 of the Table at **Appendix 2**, and scenarios 1A, 1B, 3, and 5 of the Table at **Appendix 3**. In these circumstances, the Department is not collecting personal information about individuals from the individuals concerned but, rather, from service providers. The Department can engage in 'third party collection' if the individual concerned consents to this (APP 3.6). Further, the consent of the individual concerned is required for the Department to collect sensitive information (APP 3.3(a)(i)).

4.69. Section 4 of the DSS Data Exchange Protocols document provides for standard consent arrangements for collecting a client's personal information that service providers are required to implement under grant agreements. In particular, it is stated that '[s]ervice providers must not disclose personal information to DSS or any other party without the consent of the client – specifically the names of clients attending the service or personal identifiers' (section 4.1).

4.70. As discussed above, this PIA proceeds on the basis that the Department is, or might be, collecting personal information where service providers are undertaking programme reporting by way of the web-based portal (noting that the Department is making that mechanism available to the provider to be used as a client management system for its own purposes).

4.71. According to the DSS Data Exchange Protocols document, a client's consent is required for a *service provider's disclosure* of the client's personal information to the Department (through the reporting of client-level data). Further, it is reasonably apparent from the DSS Data Exchange Protocols document that *the Department is collecting* a client's personal information on the web-based portal with the client's consent. This is because section 4.2 of that document requires service providers to 'obtain the consent of the client to record their personal information on the web-based portal'. According to that section, a 'DSS standard notification' must also be included on the registration form that service providers ask clients to complete when registering the client on the web-based portal. This notification is considered in this PIA in relation to APP 5 (see below).

4.72. According to the definition of 'consent' in section 6(1) of the Privacy Act, consent can be 'express' or 'implied'. Further, para B.35 of the APP guidelines provides that the key elements of consent are that 'the individual is adequately informed before giving consent', 'the individual gives consent voluntarily', 'the consent is current and specific', and 'the individual has the capacity to understand and communicate their consent.'

4.73. We recommend that the Department's present arrangements with service providers using the web-based portal as a client management system be enhanced to ensure that the Department is fully complying with APPs 3.3(a)(i) and 3.6 in collecting a client's personal information from those service providers. In considering what enhanced arrangements can appropriately be put in place with these service providers that will ensure that *the Department is collecting a client's personal information from service providers with the client's consent*, and having regard to points that the AIC has made about this issue in the APP guidelines (see, generally, paras B.36 to B.58), we recommend that such arrangements:

- require a service provider to obtain, on the Department's behalf, the express consent of a client for the Department's collection of his or her personal information from the provider, noting that there is a reasonable prospect that personal information that the Department collects will also include sensitive information; and
- include procedures or systems for the recording of the client's consent by the service provider (the current 'consent flag' in the web-based portal, which requires an organisation to record that it has obtained a client's consent for the handling of personal information for its own purposes, would seem to provide a useful model in this regard); and
- require that the client be informed that they may withdraw their consent at any time, and include procedures or systems for the recording by the service provider of a client's decision to withdraw their consent and the processing by the Department of that decision; and
- be designed to address the particular issues that arise with respect to the capacity of particular individuals to consent – in particular, individuals whose capacity to consent may be compromised (for example, individuals with a physical or mental disability), and children and young people (we note that the DSS Data Exchange Protocols document already recognises capacity issues in relation to children and young people (see section 2.4), and, in relation to individuals whose capacity to consent may be compromised, these issues are addressed in the DSS Data Exchange Protocols document for other purposes (see section 7.3.2 in relation to the reporting by service providers of certain voluntary extended requirements)).

Recommendation 5: Enhance present arrangements with service providers using the web-based portal as a client management system to ensure that the Department is fully complying with APPs 3.3(a)(i) and 3.6 in collecting a client's personal information from those service providers.

APP 5 - notification of the collection of personal information

4.74. According to APP 5.1, at or before the time or, if that is not practicable, as soon as practicable after, the Department collects personal information about an individual, the Department must take such steps (if any) as are reasonable in the circumstances:

- to notify the individual of such matters referred to in APP 5.2 as are reasonable in the circumstances; or
- to otherwise ensure that the individual is aware of any such matters.

4.75. The matters referred to in APP 5.2 are as follows:

- the identity and contact details of the Department;
- if the Department collects the personal information from someone other than the individual, or the individual may not be aware that the Department has collected the information, the fact that the Department collects, or has collected, the personal information and the circumstances of that collection;
- if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);
- the purposes for which the Department collects the personal information;
- the main consequences (if any) for the individual if all or some of the personal information is not collected by the Department;
- any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the Department usually discloses personal information of the kind collected by the Department;
- that the APP privacy policy of the Department contains information about how the individual may complain about a breach of the APPs, and how the Department will deal with such a complaint;
- whether the Department is likely to disclose the personal information to overseas recipients;
- if the Department is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Analysis

4.76. Section 4.2 of the DSS Data Exchange Protocols document imposes the following relevant obligations on service providers when using the web-based portal:

4.2 Additional obligations when using the web-based portal

… [T]o enable service providers to enter client data on the DSS Data Exchange web-based portal, service providers must include the DSS standard notification (as below) [on the client registration form] …

The standard notification required by DSS is:

"The information that you provide on this form includes your personal information. Your personal information is protected by law, including the Privacy Act 1988. Your personal information collected on this form is used primarily for [service provider's name]'s purposes [insert explanation of service provider's purpose and reason for collection].

As part of the services provided to you by [service provider's name], we need to collect some information about you to assist the Australian Government Department of Social Services to conduct performance reporting and research relating to the services that you receive from this organisation. To assist this process, [service provider's name] will enter your personal information onto the DSS Data Exchange web-based portal which is administered by the Department of Social Services. The Department of Social Services will not use your personal information in an identifiable form when conducting its research and evaluation, except where you have agreed or it is required by law.

You can find more information about the way the Department of Social Services will manage your personal information, including information about accessing and correcting personal information held on the DSS Data Exchange and making privacy complaints at the DSS website. For information about how [service provider's name] manages your personal information, please contact [contact information of appropriate contact in service provider]".

4.77. This PIA proceeds on the basis that information provided by a client on the service provider's registration form would include the mandatory priority requirements and, if the service provider is participating in the partnership approach, that information would also include the voluntary extended requirements.

4.78. To ensure that the Department is appropriately complying with APP 5 in collecting a client's personal information through service providers who are using the web-based portal as a client management system, we recommend that the 'DSS standard notification' be revised so that the maters notified by the Department to a client being registered by such a service provider include the following:

- that the Department is making the web-based portal available to the service provider to be used as a client management system for the provider's own purposes, and that this involves the Department storing the client's personal information on the portal for access only by the provider; and
- the APP privacy policy of the Department (in this respect, the final paragraph of the present 'DSS standard notification' could perhaps be revised to mention that more information about privacy complaints etc can be found in the Department's APP privacy policy, which has been published on the 'DSS website').

Recommendation 6: Revise the 'DSS standard notification' to ensure that the Department is appropriately complying with APP 5 in collecting a client's personal information through service providers who are using the web-based portal as a client management system.

APP 6 - use or disclosure of personal information

Use or disclosure

4.79. According to APP 6.1, if the Department holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the Department must not use or disclose the information for another purpose (the ***secondary purpose***) unless:

- the individual has consented to the use or disclosure of the information; or
- APP 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Analysis

4.80. As mentioned above in relation to APP 3, the Department collects personal information in client-unit level records from service providers who undertake programme reporting by way of the web-based portal for the purposes of making that information available ('disclosing' that information) to those providers for their own purposes. (These service providers are making use of the client management functionality of the DSS Data Exchange.) For the purposes of APP 6.1, this 'collection purpose' is clearly the Department's 'primary purpose' for collecting that information. On that basis, this PIA concludes that there is no risk that the Department is not complying with APP 6.1 in disclosing personal information to service providers in these circumstances.

4.81. Insofar as the Department uses and discloses information held by it in client-level unit records in other circumstances, the DSS Data Exchange Framework and DSS Data Exchange Protocols documents indicate that de-identified information is being used and disclosed: see, for example, section 3 of the DSS Data Exchange Framework document and section 4.3 of the DSS Data Exchange Protocols document. Provided that it is actually the case that the Department is using and disclosing de-identified information in other circumstances, or at least that there is no real risk that the information being used and disclosed could be said to be that of an individual who is reasonably identifiable (see the definition of 'personal information' in the Privacy Act), there will be no risk that the Department is not complying with APP 6.1. This is because the Department will not be using and disclosing any *personal information* that it holds for a secondary purpose.

4.82. In presently operating the DSS Data Exchange, *the Department generates particular reports* for its own use, as well as for disclosure to service providers. We have been informed that in many cases the specifications for reporting formats, which are to be predetermined, are still under development. However, the data items in these reports include, or will include, data items that have been generated by de-identifying and aggregating data items that are held by the Department in client-level unit records.

4.83. We have been provided with example copies of 'basic reports' – **Appendices 4 and 5**. The examples at **Appendix 4** can be generated within the DSS Data Exchange by a service provider in respect of the clients to whom it has provided a service, and/or employees of the Department whose duties are concerned with, for example, grant administration and policy development. The examples at **Appendix 5** can be generated only by employees of the Department. Having examined these reports, it is clear that they do not include information about individual clients who are reasonably identifiable.

4.84. Some of the example basic reports draw on mandatory priority items reported by the service provider. In particular, one such report – the 'DSS Data Exchange Organisation Summary Report (XP0031.03)' (**Appendix 4**) – presents information about the 'demographic characteristics' of a service provider's clients. The relevant data items are percentages of clients by 'age group' (which are particular age ranges), 'Indigenous Status', 'gender', 'Identification of disability/impairment/condition', 'country of birth' and 'main language spoken at home'. It is clear that the information presented here has been sufficiently de-identified and aggregated so that it is not information about any reasonably identifiable individual clients.

4.85. We have also been provided with example copies of 'infographic reports' – **Appendix 6**, which can be generated within the DSS Data Exchange by service providers participating in the partnership approach, and/or DSS employees whose duties are concerned with, for example, grant administration and policy development. These reports include data items that have been generated by de-identifying and aggregating data items that are held by the Department in client-level unit records – here, both the mandatory priority items and voluntary extended requirements that are reported by service providers are utilised. These reports also include data items that have been generated from population data sets and government data sets. In relation to government data sets, a few of the reports present percentages of a service provider's clients 'who received a welfare payment', and percentages of clients who are accessing a specified type of welfare payment.

4.86. Having examined the example 'infographic reports', it is clear that they do not, in themselves, include information about individual clients who are reasonably identifiable. There will, however, be a risk that the Department is disclosing personal information in this context if the de-identification and aggregation methods that have been used to produce a report would make it possible for a service provider to generate 'new' personal information about a client by cross-referencing a data item in a report with other information about an individual client that is already held by the provider. In this respect, and by way of example, it seems that providing a service provider with aggregate information relating to the welfare-payment status of clients, as mentioned above, would not enable the provider to establish that a particular individual client was in receipt of a welfare payment, or a welfare payment of a specified type. Of course, assessing this risk would not be relevant if the service provider already held information of this kind about the individual client.

4.87. To manage the risk that the Department might effectively be disclosing 'new' personal information about clients to service providers in the reporting context, we recommend that the Department regularly assess this risk, both in relation to reports that it presently makes available to service providers and in relation any relevant reports that will be made available to service providers in the future. In assessing this risk, the Department may wish to consult the AIC publication of April 2014 entitled 'Information Policy agency resource 1: De-identification of data and information'.

Recommendation 7: Regularly assess the risk that the Department might be disclosing 'new' personal information about clients to service providers in the reporting context.

APP 10 - quality of personal information

4.88. The Department must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the Department collects is accurate, up-to-date and complete (APP 10.1).

4.89. The Department must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the Department uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant (APP 10.2).

Analysis

4.90. As mentioned above in relation to APPs 3 and 6, the Department collects personal information in client-unit level records from, and discloses such information to, service providers who are using the web-based portal as a client management system.

4.91. As also mentioned above in relation to APP 3:

- a list of possible data values for each mandatory priority requirement data item in a client-level unit record is provided on page 44 of the DSS Data Exchange Protocols document under the heading 'Client record – mandatory priority requirements'; and
- a list of possible data values for each data item that makes up the voluntary extended requirements in a client-level unit record is provided on pages 46 to 47 of the DSS Data Exchange Protocols document under the heading 'The voluntary extended data set – the partnership approach'.

4.92. In the present context, we think that the key consideration in relation to APP 10 is whether the personal information being collected by the Department from relevant service providers, and disclosed by the Department to relevant service providers, is accurate and relevant. Given that reporting requirements for grants programme reporting effectively require service providers to report any personal information to the Department in accordance with the DSS Data Exchange Protocols document, the accuracy and relevance of personal information collected by the Department from providers, and disclosed by the Department to providers, will depend on the

nature of the reporting requirements that the Department has placed on service providers through the Protocols document.

4.93. Section 5 of the DSS Data Exchange Protocols document imposes detailed requirements on service providers in relation to collecting mandatory priority requirement data items from clients.

4.94. Many of the mandatory priority requirement data items have possible data values that are, essentially, set 'codes'. These codes, and the associated definitions, have been established by other entities (for example, the Australian Institute of Health and Welfare), and have been adopted by the Department. An example is the mandatory priority requirement that is concerned with a client's disability: see section 5.1.8 of the DSS Data Exchange Protocols document. With respect to these mandatory priority requirements, the Department will clearly be collecting and disclosing personal information that is accurate and relevant.

4.95. The other mandatory priority requirements are not set codes. In these cases, the DSS Data Exchange Protocols document includes instructions or procedures that are geared towards collecting accurate information, or an indication of the fact that the collected information is not necessarily accurate. For example, a service provider is asked to collect a client's given name by recording the given name as it appears on a key identification document: see section 5.1.1 of the DSS Data Exchange Protocols document. By way of further example, a service provider is to use a 'date of birth estimate flag' where it has collected an estimate of the client's date of birth: see section 5.1.2. The procedures and instructions in these cases also encourage the collection of accurate and relevant personal information.

4.96. Section 6 of the DSS Data Exchange Protocols document imposes detailed requirements on service providers in relation to collecting voluntary extended requirement data items from clients. The possible data values for the vast majority of these data items are set 'codes'. Again, with respect to these voluntary extended requirements, the Department will clearly be collecting and disclosing personal information that is accurate and relevant.

APP 11 – security of personal information

4.97. According to APP 11.1, if the Department holds personal information, the Department must take such steps as are reasonable in the circumstances to protect the information:

- from misuse, interference and loss; and
- from unauthorised access, modification or disclosure.

Analysis

4.98. As discussed above in relation to APP 3, authorised access to the database in which client-level unit records are held is limited to a highly restricted number of Departmental employees who perform database administration duties. These employees access this database through special accounts that have mechanisms that identify/authenticate the employees uniquely/individually. The mechanisms are

a user name and passphrase. As required by the Department's standard security practices, the passphrase must consist of a minimum length and set of characters and must be regularly changed.

4.99. The Department has also taken other specific steps to protect personal information stored, or which might be stored, in client-level unit records. As indicated in relation to scenarios 1A, 1B, 3 and 5 of the Table at **Appendix 2**, and scenarios 1A, 1B, 3, and 5 of the Table at **Appendix 3**, the client's first name and last name/pseudonym and, where it is included, full residential address (that is, 'Address Line 1 and 2') are not accessible/visible to the Department - that is, database administrators - except in exceptional circumstances. The Department has informed us that these data items are accessible/visible only for the purposes of performing specific administrative duties such as performing disaster recovery, implementing major system changes, retrieving lost or corrupted data, or troubleshooting production processing problems. The Department has confirmed that accessibility/visibility of these data items is strictly prohibited for the Department's policy or grants programme delivery purposes.

4.100. The Department's other, general steps for protecting the personal information within the Department are comprised of a comprehensive range of measures in the Department's ICT Security Policy. These measures are designed to protect the information from misuse, loss and interference, as well as unauthorised modification or disclosure. These measures include, for example, active monitoring of access to the database in which client-level unit records are stored, administering intrusion detection tools, managing audit trails, implementing procedures for data backup and recovery, and managing security patches.

4.101. The Department has informed us that these ICT Security measures are being systematically assessed and adapted to minimise security vulnerabilities in relation to the database in which client-level unit records are stored.

4.102. Grant service providers undertaking programme reporting using the DSS Data Exchange, or using the Exchange as a client management system, access the Exchange through the government authentication service known as VANguard. VANguard is a whole of government program that delivers authentication services to secure, relevantly in this case, business to government online transactions. The authentication service delivered by VANguard employs the AUSkey mechanism, which is a secure login that identifies a user when they are using the DSS Data Exchange on behalf of a service provider. The website for VANguard is http://www.vanguard.business.gov.au/Pages/default.aspx.

4.103. In relation to external measures for the protection of personal information that is held in the DSS Data Exchange, it is also relevant to mention the requirement that the Department has placed on service providers, in the DSS Data Exchange Protocols document, to notify the Department 'as soon as practical if they become aware of any security or privacy breaches': section 8.4. The Department has explained that service providers would make this notification by following procedures that are set out in grant agreements between the Commonwealth and providers.

4.104. On the information available, we have not identified any security risks to the personal information that is being managed through the DSS Data Exchange. That said, security risks need to be regularly assessed and, as mentioned above, could be appropriately assessed through, for example, an information security risk assessment.

APP 12 – access to personal information

4.105. If the Department holds personal information about an individual, generally the Department must, on request by the individual, give the individual access to the information (APPs 12.1 and 12.2). APPs 12.3 to 12.9 set out various requirements relating to requests for access, the giving of access, and refusals to give access.

4.106. The Department's obligations under APP 12 must be met in relation to the personal information (about clients of service providers) that it holds in client-level unit records in the DSS Data Exchange. However, these obligations are relevant to all of the Department's functions or activities that involve the management of personal information and, for that reason, are not given any particular consideration in this PIA.

4.107. We mention that the Department's APP privacy policy (**Appendix 1**) contains information about how an individual may access personal information about the individual that is held by the Department. As mentioned above in relation to APP 1, this policy applies to the Department's operation of the DSS Data Exchange.

APP 13 – correction of personal information

Correction

4.108. According to APP 13.1, if:

- the Department holds personal information about an individual; and
- either:
  - the Department is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or
  - the individual requests the entity to correct the information;

  the Department must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

4.109. The Department has particular obligations that relate to notifying third parties about corrections it has made (APP 13.2), refusals of requests to correct information (APPs 13.3 and 13.4), and the way in which certain requests, including requests made under APP 13.1, are dealt with (APP 13.5).

4.110. The Department's obligations under APP 13 must be met in relation to the personal information (about clients of service providers) that it holds in client-level unit

records in the DSS Data Exchange. However, these obligations are relevant to all of the Department's functions or activities that involve the management of personal information and, for that reason, are not given any particular consideration in this PIA.

4.111. We mention that the Department's APP privacy policy (**Appendix 1**) contains information about how an individual may seek the correction of personal information about the individual that is held by the Department. As mentioned above in relation to APP 1, this policy applies to the Department's operation of the DSS Data Exchange.

5. RESPONSE TO RECOMMENDATIONS

5.1. The Table in **Appendix 7** sets out the Department's response to each recommendation.

5.2. The Department has accepted recommendations 1, 2 and 7, and the Table provides an indication of how the Department intends to implement those recommendations.

5.3. The Department's response to recommendations 3, 5 and 6 reflect the fact that the Department has decided that the client management functionality of the DSS Data Exchange will be made available to service providers who report by way of a system to system transfer or bulk upload.

5.4. The Department has not accepted recommendation 4 because it has decided that there is no need for service providers to store client contact details to facilitate follow-up client surveys. In relation to this recommendation, the Table provides an indication of how the Department intends to implement this decision.

5.5. As mentioned at the bottom of the Table, in addition to responding to the recommendations that have been made, the Department has decided to limit its arrangements with service providers for protecting a client's personal information (see section 4 of the DSS Data Exchange Protocols document) to only those that are necessary to enable the Department to comply with its obligations under the Privacy Act.

6. APPENDICES

Appendix 1: Department's APP Privacy Policy (as last updated on 26 April 2016)

Appendix 2: Overview of Information Flow – Provider to DSS (Client Name & Last Name)

Appendix 3: Overview of Information Flow – Provider to DSS (Client's Pseudonym)

Appendix 4: Example copies of 'basic reports' for service providers and employees of the Department

Appendix 5: Example copies of 'basic reports' for employees of the Department

Appendix 6: Example copies of 'infographic reports'

Appendix 7: Response to Recommendations