Australian Government
Office of the Australian Information Commissioner

Handling personal information

Department of Human Services, PAYG data matching program

oaic.gov.au

OAIC

Assessment Report

Assessment undertaken: December 2017 | Draft report issued: May 2018 | Final report issued: June 2019

Contents

Part 1: Executive Summary

1.1 This report outlines the findings of an assessment of the Department of Human Services' (DHS) Pay-As-You-Go (PAYG) data matching program, undertaken by the Office of the Australian Information Commissioner (OAIC).

1.2 The scope of this assessment was limited to considering DHS's handling of personal information for the purposes of the PAYG program under Australian Privacy Principle (APP) 10 (quality of personal information) and APP 13 (correction of personal information).

1.3 The assessment found that DHS has taken some steps to address issues with the quality of the personal information it collects and uses and has implemented many changes to the PAYG program following an investigation by the Commonwealth Ombudsman (Ombudsman) in early 2017.

1.4 However, the OAIC also identified potential privacy risks associated with the PAYG program and has made five recommendations to address these risks. The OAIC recommended that DHS:

- implements additional measures to ensure the personal information it receives from the ATO for the PAYG program **is accurate, up-to-date and complete**, having regard to the purposes for which the personal information is being used. Such measures could include entering into a more formal arrangement, such as a Memorandum of Understanding with the ATO as a way of dealing with the management of personal information, including personal information quality issues that arise specifically under the PAYG program.
- addresses the **quality of the personal information** that it uses in its PAYG program by:
    - reviewing, and if necessary, improving the data validation techniques it employs at the point of data entry, i.e. when DHS staff enter a customer's personal information into DHS systems
    - implementing a regular audit or quality assurance program to examine customer records used in the PAYG data matching program to ensure the information in those records is complete, accurate and up-to-date
    - reviewing its staff training to ensure it addresses personal information quality issues and to ensure personal information quality is understood by staff to be a privacy issue.
- in relation to the Employment Income Confirmation (EIC) process:
    - implements additional measures to facilitate **customer-initiated correction** of information under the EIC process to ensure the outcome of the EIC process, following review by customers, is that any debt calculation is based on accurate, up-to-date and complete information
    - makes automated and manual compliance intervention processes as **easy as possible** for customers to understand and use. The EIC process should clearly communicate to customers what information they are being asked to review and how to obtain the correct information to input into the system if required.

- implements measures to ensure it is adhering to the minimum procedural requirements in relation to **correcting personal information** contained in APP 13 (specifically 13.2-13.5), whenever a customer raises concerns about their personal information being incorrect, including during the EIC compliance intervention process.
- in relation to **privacy threshold assessments** (PTAs):
    - continues to conduct PTAs, and where appropriate, privacy impact assessments (PIAs), for any future changes to the PAYG program
    - considers including specific questions about personal information quality as part of its PTA form to raise awareness of the possible privacy implications of poor quality personal information, and ensuring personal information quality is also captured by the PIA process
    - monitors the implementation of any recommendations that arise out of such assessments.

Part 2: Introduction

Background

2.1 The Department of Human Services (DHS) undertakes a range of compliance activities through data matching programs to ensure ongoing eligibility for entitlements and to maintain the integrity of customer payments and services.

2.2 Data matching is the bringing together of at least two data sets that contain personal information from different sources, and the comparison of those data sets with the intention of producing a match.[1] Agencies must comply with the *Privacy Act 1988* (Privacy Act) and this encompasses the data matching related activities that they undertake.

2.3 The Office of the Australian Information Commissioner (OAIC) has been funded to provide regulatory oversight of privacy implications arising from DHS's increasing data matching activities using new methodologies, for the period from 1 January 2016 to 30 June 2019. This funding is part of the 'Enhanced Welfare Payment Integrity – non-employment income data matching' 2015-16 budget measure.

2.4 DHS conducts a number of data matching programs to determine whether a customer's payments are accurate based on the type of income customers earn or the payments they receive. Information about an individual's income, when combined with other information such as name and address, is personal information for the purposes of the Privacy Act.

2.5 The Pay-As-You-Go (PAYG) program matches PAYG taxation data from the Australian Taxation Office (ATO) with information that DHS collects from customers about their income. The PAYG program began with a pilot program in 2001, and formally commenced in 2004.

2.6 The purpose of the PAYG program is to identify non-compliant customers requiring administrative or investigative action. The PAYG program focuses on identifying discrepancies between the employment income that customers report to DHS and the PAYG payment summary information that employers provide to the ATO.[2]

Overview of the PAYG program

2.7 On 1 July 2000, the ATO introduced PAYG as a single integrated taxation system for reporting and paying withholding amounts and tax on business and investment income. In the 2000-2001 Budget, a pilot data matching program using information generated from this system was announced. The pilot program compared a customer's Centrelink income details with their ATO PAYG payment summaries and, where discrepancies were identified between the DHS and ATO figures, DHS undertook further review of the customer's records.

[1] Office of the Australian Information Commissioner Guidelines on Data Matching in Australian Government Administration June 2014, Key terms section.
[2] Department of Human Services, Pay-As-You-Go (PAYG) Data-Matching program protocol , May 2017, p.4.

2.8 Following the pilot, the PAYG program was rolled out in 2004. Since that time, DHS and the ATO have continued to exchange customers' personal information for the purposes of identifying discrepancies in recorded employment income data.[3]

2.9 Under the PAYG program DHS provides the ATO with certain personal information about a customer and the ATO then uses that information to match against its own records. The ATO assesses possible matches according to its own internal rules, and if a match meets a certain confidence rating, the ATO sends DHS the PAYG payment summaries for the person related to the matched record.

2.10 Once DHS receives this information from the ATO, it follows certain internal processes to decide whether to take further compliance action in relation to such discrepancies in reported employment income, including raising debts against customers.

2.11 Prior to July 2016, the data matching and debt raising processes using PAYG information were undertaken manually. If the data matching process identified a potential overpayment, then a compliance officer would contact the customer, requesting further information from them, and would remain involved throughout the compliance process.

2.12 After a two-stage pilot in 2015, an automated Online Compliance Intervention (OCI) process was launched with a limited rollout in July 2016, followed by a wider rollout in September 2016. An online OCI portal was also launched to allow customers to review, and then confirm or amend, their information as part of the compliance process. DHS made a number of changes to the OCI process and customer communication methods following negative customer feedback and a subsequent Ombudsman's investigation in early 2017. These changes included improvements to the OCI customer portal and the letters sent to customers. The automated process was also renamed the Employment Income Confirmation (EIC) process.[4]

2.13 The automated process and online customer portal will be referred to as the EIC process or portal throughout this report, except where the reference is specifically made to the former OCI process or portal.

2.14 Further information about the history of the PAYG program, its previous manual process, as well as earlier versions of the OCI process, is available in Appendix A of the Ombudsman's report, *Centrelink's automated debt raising and recovery system* (Ombudsman's report). Appendix B of that report also provides more detail about the OCI in operation.

2.15 A summary of the flow of personal information through the PAYG data matching program, including the current EIC process, is described in Table 1 below. The OAIC obtained this information based on advice from DHS and review of relevant documents.

[3] For more information about DHS's PAYG data matching program, see the Pay-As-You-Go (PAYG) Data-Matching Protocol May 2017.

[4] The OAIC understand that, in the time since this assessment was conducted, a new online portal, called Check and Update Past Income (CUPI), went live in October 2018. We understand that this is running concurrently with the EIC until the phase out of the EIC is complete. See *Centrelink's automated debt raising and recovery system – implementation report* (Ombudsman follow-up report), published April 2019, page 14.

Table 1

Flow	Process	Description
1	Collection (DHS)	The customer provides information to DHS in order to receive various services and payments. This is discussed in further detail at paragraph 3.30 below.
2	Disclosure (DHS)	DHS provides the ATO with the following data items for identity matching purposes: • DHS Customer Reference Number (CRN) • full name (including any known aliases) • gender • full address, including historical addresses • date of birth.
3	Collection/Use (ATO)	The ATO uses its proprietary software to identity match the DHS customer information with ATO records.
4	Collection (DHS)	Where the ATO determines that a match reaches a requisite confidence level, then the ATO will send the following data items to DHS: • PAYG payment summary – payer record • PAYG payment summary – payee record.
5	Collection/Use (DHS)	When DHS receives the matched data from the ATO, DHS conducts some validation of the data received to ensure it relates to the correct customer. The validation process is discussed at paragraphs 3.8-3.13. Once this validation process has taken place, DHS then: • identifies customers who have a discrepancy between the income they have declared to DHS and the income recorded in their PAYG payment summaries • uses internal business rules to assess the risk that the customer is potentially non-compliant and therefore to determine whether to begin compliance action, including: o as a minimum, the customer must be receiving, or have been in receipt of, a suitable payment type and a minimum amount of income o the likely level of income discrepancy.

Flow	Process	Description
		• enters compliance cases selected for action into an online management system, ready to be initiated • applies filters to either temporarily defer or exclude cases that are flagged with particular markers, including customers identified as vulnerable,[5] people in prison, deceased people, and customers living in declared disaster zones during the period of the disaster and for an appropriate period afterwards • starts the automated compliance process, which creates an initial letter to each of the selected customers • sends the initial letter to selected customers either by registered post or online through their myGov account. Both of these options produce a receipt to confirm the customer has received the letter • sends the initial letter by registered post if a customer does not open an online letter within 14 days • contacts the customer by phone to obtain their correct address if a letter is returned unopened to DHS. If a current addressed cannot be obtained, then the compliance process ends.
6	Collection (DHS)	Upon receipt of the letter, customers may update their information, either online or to a DHS compliance officer in person or by telephone. • customers have 28 days from first logging into the online portal to complete the compliance process • a reminder letter is sent by registered post 14 days before the expiration of the 28 day period if a customer has not completed the process • a further reminder is sent on the due date, which grants a 14 day extension (taking the total period to 42 days) • if the due date passes and a customer has not completed the process, then a staff member will attempt to contact them twice by telephone • customers who are unable to meet the timing requirements can request a further extension online or by calling DHS.

[5] Some of these markers, such as the one for vulnerable people, have been introduced or modified since the release of the Ombudsman's report.

Flow	Process	Description
7	Use (DHS)	If a customer has started the compliance process but has not completed it by the extended due date (i.e. minimum period of 42 days), and DHS cannot contact the customer after two telephone attempts, then DHS will use the best available data to calculate whether the customer owes a debt. DHS may apply a 10% debt recovery fee to a compliance case that has reached this point. DHS uses an averaging process on the ATO PAYG payment summary information. This means that the amount a customer has earned from a particular employer is evenly divided across the number of fortnights that the customer worked for that employer. For example, where a customer has worked for an employer for 6 months, the total amount recorded on the payment summary for that employer is divided by the 13 fortnights in that 6 month time period. As eligibility for many DHS payments is determined on a fortnightly basis, such averaging will directly impact on a determination of whether a customer has 'accurately' declared their income and therefore whether they owe a debt. DHS then sends a notice of decision letter to the customer advising them of whether they have a debt.
8	Disclosure	In some circumstances, such as instances of fraud or other criminal activity, DHS may refer a customer's matter to the Commonwealth Director of Public Prosecutions for further action.

Part 3: Findings

Our approach

3.1 The key findings of the assessment are set out below under the following headings:

- Personal information quality and correction – DHS collection from the ATO
- Personal information quality and correction – use of DHS records
- Personal information quality and correction – customers
- General privacy issues

3.2 For each issue, we have summarised the OAIC's observations and the privacy risks arising from these observations, followed by suggestions or recommendations to address those risks.

3.3 The OAIC has considered the:

- APP Guidelines, which outline the mandatory requirements of the APPs, the way in which the OAIC will interpret the APPs and matters the OAIC may take into account when exercising functions and powers under the Privacy Act in the privacy analysis below
- Guidelines on Data Matching in Australian Government Administration (the Data Matching Guidelines), which aim to assist Australian Government agencies to use data matching as an administrative tool in a way that complies with the APPs and the Privacy Act and is consistent with good privacy practice.

3.4 As noted above at paragraph 2.12, the Ombudsman conducted an investigation into the OCI system for debt raising and recovery and published a report of its findings in April 2017. The OAIC decided to delay an assessment of the PAYG program until the Ombudsman's investigation and report were completed so that the findings could inform the OAIC's assessment. The OAIC has considered the observations and recommendations made in the Ombudsman's report, where appropriate.

3.5 Throughout this report, APPs 10 and 13 will generally be considered together. Under APP 10, DHS must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, up-to-date, complete and relevant, having regard to the purpose for which it uses the information. Alongside this obligation is the requirement under APP 13 for DHS to take reasonable steps to correct personal information to ensure that it is up-to-date, complete, relevant and not misleading, having regard to the purposes for which it uses the information. DHS must take such steps if either an individual requests a correction, or where DHS becomes aware that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

Personal information quality and correction – information collected from the ATO

Observations

3.6 As outlined in Part 2 of this report, one of the data sets used in the PAYG data matching program comes from the ATO. DHS discloses to the ATO certain personal information about a customer and the ATO runs the identity matching process on its proprietary software. DHS discloses this information to the ATO twice each financial year – in November and May – to ensure it receives PAYG summaries submitted by late-lodging employers. The OAIC did not assess the ATO's role in the PAYG program, or its data matching processes, during this assessment.

3.7 DHS receives data that falls within the ATO's top two or three confidence ratings,[6] which the ATO applies based on its assessment of the reliability and accuracy of the data. DHS staff interviewed during fieldwork were not aware of the ATO's method for determining these ratings.

3.8 Once it receives the matched data from the ATO, DHS conducts checks on the data to ensure the data is in a matchable format. For example, names and addresses must appear in the correct fields.

3.9 DHS explained that data errors are quite common in the ATO's PAYG payment summary data because the information is entered into the PAYG system by employers. In particular, DHS regularly encounters errors in the dates that employers recorded. However, as the ATO uses the information to calculate annual tax obligations, many of these errors are irrelevant for the ATO's purposes.

3.10 DHS advised that it may amend a date recorded in an incorrect format in the PAYG payment summary, in accordance with its internal business rules.

3.11 DHS also employs some 'fuzzy logic'[7] rules to overcome other discrepancies in the ATO data, which DHS has determined to represent no or low risk. An example of this is where two employer names are the same, but one of them includes 'Pty Ltd' after the name and the other does not.

3.12 In addition, DHS advised that some data errors, reported by customers after they received a letter from DHS, related to identity mistakes that can be traced back to the TFNs used by the ATO during the data matching process. These mistakes generally arise from TFN misuse by an employee or an employer or are a case of mistaken identity between family members.

3.13 DHS's data validation also includes high-level checks to ensure the matched data received from the ATO actually corresponds to the correct customer. The check includes the customer's CRN, and at least either their name, address or date of birth. Following this

[6] During fieldwork, DHS staff were unsure whether the ATO sends the top two or three confidence ratings. The Commonwealth Ombudsman's report (p. 39) notes that DHS advised that it is the top three confidence levels that are provided.
[7] This is the term used in the Commonwealth Ombudsman's report (p. 40, paragraph 2.17), which describes fuzzy logic as "a set of rules for ignoring certain discrepancies based on the probability that they are no or low risk."

validation, DHS typically identifies approximately 40,000 non-matches, mismatches, or multiple matches. DHS then withdraws these records from the automated EIC process and manually checks them for a correct match.

3.14 If a match passes DHS's validation and fuzzy logic checks, then the compliance action process outlined in Table 1 continues. In circumstances where the customer has started the compliance process but has not completed it by the due date, and DHS cannot contact the customer after two telephone attempts, then DHS will apply averaged ATO data (see flow 7 in Table 1 above) to calculate whether the customer owes a debt. DHS advised that it did not hold any data in relation to how often averaged ATO income data is used to determine a debt.

3.15 Before the introduction of the OCI system, only customers with the highest risk rating were selected for compliance action. The OCI/EIC system has expanded the compliance program to include customers with lower risk ratings.

3.16 The relationship between DHS and the ATO for the purposes of the PAYG program has been formally in place since the program rolled out in 2004. DHS and the ATO also cooperate on a variety of other data matching programs. The two agencies have a number of high-level arrangements in place, including a general head agreement to manage their relationship, as well as a specific data exchange service schedule and a related arrangement to manage the exchange of data between the two agencies, which include references to the data exchanged for the PAYG program. These written agreements are complemented by a governance committee and a data management forum.

3.17 However, when asked about any specific arrangements in place to manage the PAYG data matching program, DHS advised that the program operates on an implied level of trust between the two agencies.

3.18 During fieldwork, DHS staff advised that in situations where DHS identifies an error in the ATO data, the error is corrected for DHS's purposes, but is not communicated to the ATO. Data errors are only communicated to the ATO in situations where an individual alerts DHS to a potential error and DHS is unable to resolve it.

Analysis

3.19 To meet its obligations under APPs 10 and 13, DHS must take reasonable steps to ensure it maintains the quality of its personal information holdings. This includes employing appropriate oversight over a third party from whom personal formation is collected, and correcting personal information where DHS is satisfied, independently of any request from an individual, that the personal information does not meet the requirements of APP 10.

3.20 As noted above, DHS staff acknowledged that there is a personal information quality issue posed by the ATO data, particularly because of the different purposes for which the personal information was collected. A DHS-commissioned review of the EIC also highlighted this issue and noted that there is no system of governance from the ATO to ensure employment information is accurate.

3.21 To address this problem, DHS has put in place some internal measures, such as business rules for amending dates and conducting basic validation checks to ensure the data facilitates the compliance activities undertaken for the PAYG program. However, DHS does not seek to verify the accuracy of the ATO data and, instead relies on individuals to verify the

accuracy of the data via the EIC system (see 'Personal information quality and correction – customers' section below).

3.22 DHS's current practices in relation to the ATO's personal information raise concerns about the steps DHS is taking to ensure the personal information is accurate and fit for purpose, as well as the processes DHS employs to correct personal information.

3.23 The averaging of a customer's annual income across fortnightly periods in circumstances where the customer cannot be contacted or does not respond raises a risk that debt calculations may be based on inaccurate information resulting in miscalculated debts. For example, the averaging process may not accurately reflect income earned by customers with varying employment arrangements for example casual workers and contractors.

3.24 Further, while inaccurate dates recorded on payment summaries may not affect annual tax obligations, they can pose problems for accurately determining whether a discrepancy exists between DHS's and the ATO's data sets. As the EIC process requires customers to confirm their income on a fortnightly basis, errors in the PAYG payment summary dates can compound a personal information accuracy issue when calculating a possible discrepancy.

3.25 In addition, DHS has little knowledge or oversight over the ATO's processes associated with the PAYG program.

3.26 In the OAIC's view, these issues present a medium risk that potential personal information quality issues are not being identified, or if they are, that mechanisms do not exist to ensure personal information quality issues are being addressed in a timely and comprehensive manner.

3.27 To address this risk, the OAIC recommends that DHS implements additional measures to ensure the personal information it receives from the ATO for the PAYG program is accurate, up-to-date and complete, having regard to the purposes for which the personal information is being used. While DHS and the ATO have some high-level arrangements in place to manage their general data matching relationship, a formal arrangement with the ATO at a program level, for example through a Memorandum of Understanding, would help DHS and the ATO deal with the management of personal information, including personal information quality issues that arise specifically under the PAYG program.

3.28 Such an arrangement can facilitate PAYG-specific discussions around personal information management and set out mechanisms between both agencies for raising and addressing personal information quality issues. For example, a formal feedback mechanism could be introduced so that the ATO is made aware of instances where DHS is altering dates on payment summaries, which may help the ATO to identify data errors that are occurring. Having a formal arrangement may also help to preserve corporate knowledge of the PAYG data matching process within and between both agencies.

3.29 We note that DHS's response to data breaches is outside the scope of this assessment, and that the Notifiable Data Breaches (NDB) scheme[8] commenced after the fieldwork for this assessment.[9] However, when preparing a formal arrangement to govern the PAYG program,

[8] For more information about the NDB scheme, see https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.

[9] The NDB scheme commenced 22 February 2018, whilst fieldwork for this assessment occurred on 12 and 13 December 2017.

DHS and the ATO should consider and document how they will coordinate a response in the event that any personal information used in the PAYG program is subject to an eligible data breach.[10]

Recommendation 1

The OAIC recommends that DHS implements additional measures to ensure the personal information it receives from the ATO for the PAYG program is accurate, up-to-date and complete, having regard to the purposes for which the personal information is being used. Such measures could include entering into a more formal arrangement, such as a Memorandum of Understanding with the ATO as a way of dealing with the management of personal information, including personal information quality issues that arise specifically under the PAYG program.

Personal information quality and correction – use of DHS records

Observations

3.30 In addition to the ATO data set, DHS uses its own customer records in the PAYG data matching program. This information primarily comes from customers themselves, when they apply for certain programs and services and throughout the duration of their engagement with DHS. Customers provide information using hard copy or online forms, by telephone, or in person and DHS staff enter it into the relevant database.

3.31 DHS also draws some customer information from external sources. For example, DHS receives notifications of customer deaths from State and Territory Births, Deaths and Marriages offices, and information on customers' overseas travel from the Department of Immigration and Border Protection.[11]

3.32 DHS advised the OAIC of its personal information quality issues, including intertwined Centrelink records[12] and customers with more than one CRN. DHS has identified approximately 250,000 duplicate CRNs across its records, though instances of intertwined Centrelink records are relatively limited. DHS has a data quality team, who work to remedy intertwined records for both Centrelink and Medicare, as well as issues relating to multiple CRNs. DHS advised during fieldwork that the focus of the data quality team, at the time of the assessment, was on intertwined records rather than on duplicate CRNs.

[10] For information about responding to a data breach, see the OAIC's Data breach preparation and response - A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth). In particular, consider the section on 'Data breaches involving more than one entity'.

[11] Subsequent to this assessment being conducted, the Department of Home Affairs was established and carries out the functions of the former Department of Immigration and Border Protection.

[12] An intertwined record is a single Centrelink enrolment record that has been used interchangeably between two or more individuals.

3.33 The quality of DHS's personal information relies on its staff to accurately enter data into customer databases, as well as customers to provide updates to their individual circumstances. All DHS staff receive general training on security, privacy and misuse of information during induction training. Staff also receive annual privacy refresher training as part of their Individual Performance Agreement. In addition, staff working on the PAYG program compliance telephone line receive specific training on using the EIC system. When major changes to that system occur, DHS provides staff with additional training. Minor changes are communicated to staff through other channels, such as regular newsletters and quality development officers.

3.34 While DHS advised that training addresses the impact of poor quality data on the outcome of a decision, this is not framed as a privacy issue or directly covered in privacy training. DHS also advised that training does not address the issue of multiple CRNs being created, or ways to remedy this.

3.35 DHS advised that it conducts a number of department-wide compliance activities to check the accuracy of customer's entitlements. An example includes conducting rolling random sample surveys to identify whether customers are receiving the correct payments or services. However, these compliance activities are not linked to PAYG or other data matching programs even though they could be and are therefore not used to monitor or improve personal information accuracy for these programs.

3.36 DHS also advised the OAIC that it is conducting some data mining and data analytics activities but these activities, at the time of the assessment, had limited impact on the PAYG program.

Analysis

3.37 In accordance with its obligations under APPs 10 and 13, DHS must take reasonable steps to ensure it maintains the quality of its personal information holdings, including correcting that information when it becomes aware that it is inaccurate.

3.38 DHS staff are aware of the role that human error plays in creating instances of customers with multiple CRNs. While the approximate figure of 250,000 duplicate CRNs is across DHS, some of these customers would be captured by the compliance activities of the PAYG program. This means that there is a medium risk that DHS is conducting compliance activities against customers with duplicate or multiple CRNs, and in doing so, could be using inaccurate, out of date, or incomplete information to determine possible debts.

3.39 Human error is regularly identified to be a significant cause of privacy incidents;[13] consequently DHS should assume that human error will occur and design for it in its programs and systems.[14] Research has shown that human error can be seen as a trigger rather than a cause of an incident.[15]

---

[13] In the OAIC's first quarterly Notifiable Data Breaches scheme statistics report for the period January-March 2018, 32 of 63 data breach notifications received by the OAIC were caused by human error.

[14] See the Own motion investigation report AICmrCN 5. This case illustrates how the failure to put in place adequate policies, procedures and systems to mitigate the risk of human error can result in a data breach. Failures at a number of levels aligned to create circumstances that enabled a breach to occur.

[15] This approach is based on the 'Swiss cheese' or 'cumulative act effect' model of accident causation which is an illustration of how organisational failures at a number of levels can combine to create a situation in which human error

3.40 To mitigate the risk of poor quality personal information, the OAIC recommends DHS reviews, and if necessary, improves the data validation techniques it employs at the point of data entry, i.e. when DHS staff enter a customer's personal information into DHS systems. Such controls could include setting parameters on data entry fields and implementing certain algorithms to reject questionable data. DHS could also consider utilising user prompts during data entry to flag that a customer may already have a CRN.

3.41 DHS should also regularly audit, identify and correct poor quality personal information. For example, DHS should consider implementing a regular audit or quality assurance program to examine customer records used in the PAYG data matching program to ensure the information in those records is complete, accurate and up-to-date. The audit would also assist with reducing instances of customers with multiple CRNs.

3.42 In addition, DHS could consider leveraging existing departmental information quality monitoring measures, such as its rolling random sample surveys, to more proactively monitor the accuracy of the personal information it uses in the PAYG data matching program. Where personal information quality issues are identified, DHS could consider additional measures to address these issues.

3.43 To support these personal information quality measures, DHS should also review its existing privacy and EIC-specific training to ensure it includes personal information quality and correction issues, including the importance of accurate data entry as a means of avoiding duplicate records and other data errors. This training should be provided to a range of staff, including those on the EIC telephone helpline, as well as all staff who are involved in the entry of customer data into DHS databases, including general telephone and customer service staff.

Data analytics

3.44 Data analytics involves amassing, aggregating and analysing large amounts of data.[16] Where data analytics involves personal information, DHS must ensure it is complying with the requirements of the Privacy Act.

3.45 Based on discussions with staff during fieldwork, there is potential for DHS's data mining and data analytics activities to expand and begin to interact with the compliance activities of the PAYG program.

3.46 Ensuring accuracy and quality in data analytics is particularly important where information may be used to make business decisions that affect an individual. If DHS's use of data analytics increases, and particularly if this extends into data matching programs such as the PAYG program, it would be prudent for DHS to consider whether it should take additional and more rigorous steps to ensure the quality of both the personal information collected, as well as any additional personal information created by the algorithms that process the data. Such steps could include the personal information quality measures discussed at 3.40-3.43 and conducting privacy threshold assessments (PTA) and privacy impact assessments

---

can trigger a data breach. This is a model used in risk analysis and risk management originally propounded by Dante Orlandella and James T. Reason in 1990.

[16] Data analytics is a broad and evolving term. It covers concepts such as 'big data', 'data integration', data mining' and 'data matching'. For more information, see the OAIC's Guide to Data Analytics and the Australian Privacy Principles at Part 1.2.

(discussed below), in order to adequately cover personal information quality issues in its data analytics activities.

3.47 For more information about the impact that data analytics can have on the quality of personal information an entity holds, as well as examples of reasonable steps that may be appropriate for an entity to take to minimise these impacts, see Part 2.7 of the OAIC's Guide to Data Analytics and the Australian Privacy Principles.

Recommendation 2

The OAIC recommends that DHS addresses the quality of the personal information that it uses in its PAYG program by:

- reviewing, and if necessary, improving the data validation techniques it employs at the point of data entry, i.e. when DHS staff enter a customer's personal information into DHS systems
- implementing a regular audit or quality assurance program to examine customer records used in the PAYG data matching program to ensure the information in those records is complete, accurate and up-to-date
- reviewing its staff training to ensure it addresses personal information quality issues and to ensure personal information quality is understood by staff to be a privacy issue.

Personal information quality and correction – customers

Observations

Changes following the Ombudsman's investigation

3.48 In April 2017, the Ombudsman published a report of its findings following an investigation into the debts raised by the OCI (now known as the EIC) system. Customer complaints made to the Ombudsman, as well as media scrutiny and complaints from community stakeholders, prompted this investigation. Many of these complaints were made in late 2016 and early 2017, following the rollout of the OCI system in July 2016.[17]

3.49 As part of that report, the Ombudsman made eight recommendations, many of which centred on DHS's communication to customers.[18] These recommendations identified barriers for customers in seeking to understand, interact with, and input information into the OCI system. They included communication to customers through the contact letters sent to them, the messaging within the OCI portal itself, the ease with which some customers could obtain employment income evidence to update the information in the OCI system, and the

[17] For more information about the Ombudsman's decision to undertake its investigation, see Part 1 of the Ombudsman's report.
[18] The Ombudsman's recommendations are summarised in Part 4 of the report.

resources available to customers to understand how to use the OCI system. In addition, the report noted the particular difficulties for vulnerable customers.[19]

3.50 Many of these recommendations are also relevant to understanding how DHS complies with its obligations under the Privacy Act, particularly APPs 10 and 13. Therefore, as part of this assessment, the OAIC considered the Ombudsman's recommendations, reviewed documents provided to the Ombudsman as evidence of the implementation of these recommendations, and interviewed staff who were involved in this process. The OAIC found that DHS has implemented many changes to the PAYG program following customer complaints and feedback from the Ombudsman. A range of improvements were made as part of the February 2017 changes to the OCI, which was also renamed the EIC at the same time. Other changes have been made following the Ombudsman's report in April 2017, with further changes planned following fieldwork.[20].

3.51 Examples of changes already implemented at the time of fieldwork include using registered post receipts or online read receipts to confirm that customers have received the initial letter asking them to confirm their employment income,[21] and increasing the number of filters to exclude certain cohorts of vulnerable, or potentially vulnerable, people from the current compliance program until DHS has developed appropriate methods of engaging with them.[22] DHS has also updated the information about how the EIC process works on its website.[23]

3.52 As part of the changes made in February 2017, DHS also introduced an additional method for customers to access the EIC online portal. Previously, customers had to have, or create, a myGov account to access the EIC online portal. Customers can now access the portal either through their myGov account, or through another authentication pathway with a code that is sent to the customer in their initial letter.

3.53 In preparation for anticipated changes to the EIC, DHS has also taken steps to engage third party assistance to review its processes and identify additional areas for improvement. During fieldwork, DHS staff advised that it was conducting pilot testing of changes to the EIC process and portal to improve customer engagement with the process. This testing had a particular focus on older customers' engagement, as well as on the notification process and usability of the EIC portal.

Further areas for improvement

3.54 Whilst many changes have been made, the OAIC observed possible further areas for improvement, which should assist customers to correct the information that DHS holds about them, and in turn improve the quality of personal information that DHS uses to determine whether to take compliance action against a customer.

---

[19] Examples of vulnerable customers given in the Ombudsman's report (p.19) include those "who face challenges such as remoteness, a lack of literacy, lack of English, disability, or homelessness."

[20] In the time since the assessment, the Ombudsman has published a follow-up report, *Centrelink's automated debt raising and recovery system – implementation report*, which sets out the extent to which the Ombudsman considers its original recommendations have been implemented and makes four further recommendations.

[21] This relates to recommendation 2 of the Ombudsman's report.

[22] This relates to recommendations 6 & 7 of the Ombudsman's report.

[23] For example, the DHS webpage with information about the EIC process now includes a video explaining how the process works - https://www.humanservices.gov.au/individuals/subjects/employment-income-confirmation. This relates to recommendation 5(b) of the Ombudsman's report.

3.55 During fieldwork, DHS demonstrated to the OAIC the online customer-facing portal that a customer logs in to following receipt of the initial letter from DHS.

3.56 After viewing each of the screens, the OAIC noted some areas of concern. For example, some screens within the system used technical language instead of plain English. Other screens stated that income information was provided by the ATO but did not explain that this information is drawn from a PAYG payment summary provided to the ATO by the individual's employer. While the cohort of potentially vulnerable people had been expanded since the time of the Ombudsman's investigation, there were still issues around accommodating customers who may have difficulty understanding the process, such as those requiring translation services.

3.57 In addition, the averaging process (explained above in Part 2, Table 1) was not explained in the EIC portal. One of the screens contained a statement that if the information was not confirmed within a specified time period, then DHS 'will apply the information from the ATO to your record and this may result in a debt. For more detail on how the information is applied, go to www.humanservices.gov.au/compliance.'

3.58 During the demonstration of the EIC process, DHS also highlighted the many points at which a particular answer would prompt a manual handoff to a compliance officer, resulting in the transfer of a customer from the automated process to a manual one. Following the Ombudsman's investigation, DHS commissioned a review of the process, which found that up to 97% of compliance actions involved manual intervention. This statistic, along with other findings in that review, indicates the difficulties customers continue to face in interacting with the automated online system to confirm or correct their personal information, as well as the inability of the EIC process to fully accommodate many of the variables that can arise out of each customer's unique circumstances and experience.

APP 13 procedural requirements

3.59 Under APP 13, DHS has specific obligations in relation to steps it must take if a customer makes a request for their personal information to be corrected. If DHS refuses any such request, these obligations also include providing a written notice to a customer[24] and taking reasonable steps to associate a statement with the personal information that the customer believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading.[25]

3.60 DHS advised that a process is in place to comply with APP 13. This process applies when DHS receives a request or a formal privacy complaint relating to correction of personal information through its privacy complaints channels. During fieldwork, the OAIC asked DHS staff whether DHS complies with these requirements when a customer, who is interacting with a staff member as part of a manual compliance process, advises that their information is incorrect, but DHS staff considered it inappropriate to alter the information under such a circumstance. However, DHS advised that EIC staff did not know about their privacy obligations when a customer requested to have their personal information corrected.

[24] See APP 13.3
[25] See App 13.4.

Analysis

3.61 While DHS has made many changes to the EIC system and associated processes since the Ombudsman's investigation, there remain areas for improvement in how DHS communicates with customers.[26] Clear communication ensures that customers understand what information they are being asked to confirm, where DHS has sourced their personal information from, how customers can check if the information is correct, and how to gather and provide evidence to DHS if they think it is incorrect.

3.62 Based on the information provided to the OAIC at the time of this assessment, the OAIC identified some areas that could be confusing for customers and may prevent customers from being able to adequately engage with the PAYG compliance process. This could lead to a decision on whether a customer owes DHS a debt being based on poor quality personal information. Without further improvement to make the PAYG compliance processes more user-friendly, there is a medium risk that DHS will use poor quality personal information to calculate debts.

3.63 Therefore, the OAIC recommends that DHS implement additional measures to facilitate customer-initiated correction of information through the EIC process. DHS should take all reasonable steps to ensure the outcome of the EIC process, following review by customers, is that any debt calculation is based on accurate, up-to-date and complete information. In particular, all automated and manual compliance intervention processes should be as easy as possible for customers to understand and use. The EIC process should clearly communicate to customers what information they are being asked to review and how to obtain the correct information to input into the system, if required.

3.64 Based on the version of the online portal that the OAIC viewed during fieldwork, DHS should revise the information in this portal to use plain English. DHS should also clarify that the ATO information is drawn from PAYG summaries provided by the customer's employers, so that customers can check their own records and can liaise with the ATO and employers if necessary, to correct other sources of the same information. Importantly, DHS should clearly explain in the EIC portal, in plain English, how it averages and uses the ATO's income data to determine whether a debt is owed.

3.65 In addition, at the time of the assessment, letters provided to customers did not include any information about accessing translation services. However, DHS staff noted during fieldwork that language requirements are clearly identified in a customer's file. The OAIC therefore recommends that DHS review its engagement with non-English speaking customers through the PAYG program and the EIC process. As a minimum, DHS should consider including contact information for the Translating and Interpreting Service in its letters, and in other forms of communication.

3.66 The OAIC is aware that further changes to the EIC system were scheduled to occur after the assessment. With this in mind, the OAIC suggests that DHS continues to test and evaluate any changes to customer communication methods, including letters, telephone scripts, and the online portal, so that these methods of communication promote customer

[26] This is also reflected in the four further recommendations made in the Ombudsman's follow-up report. See pages 28-29 of *Centrelink's automated debt raising and recovery system – implementation report*.

understanding and ease of interaction with both the automated and manual compliance processes.

3.67 In addition, there is a risk that DHS is not meeting the minimum procedural requirements in APPs 13.2-13.5 if a customer raises concerns about their personal information being incorrect during the EIC compliance intervention process. DHS should implement measures to ensure compliance with these minimum procedural requirements in APP 13 whenever a customer raises concerns about their personal information being incorrect, including during the EIC compliance intervention process.

Recommendation 3

The OAIC recommends that DHS:

- implements additional measures to facilitate customer-initiated correction of information under the EIC process to ensure the outcome of the EIC process, following review by customers, is that any debt calculation is based on accurate, up-to-date and complete information
- makes all automated and manual compliance intervention processes as easy as possible for customers to understand and use. The EIC process should clearly communicate to customers what information they are being asked to review and how to obtain the correct information to input into the system if required.

Recommendation 4

The OAIC recommends that DHS implements measures to ensure it is adhering to the minimum procedural requirements in relation to correcting personal information contained in APP 13 (specifically 13.2-13.5), whenever a customer raises concerns about their personal information being incorrect, including during the EIC compliance intervention process.

General privacy issues

Observations

Privacy threshold assessments and privacy impact assessments

3.68 DHS's operational privacy policy requires its staff to undertake a privacy threshold Assessment (PTA) for all new projects, or changes to existing projects, which involve the collection, storage, access to, use, disclosure or alteration of personal or protected information. The PTA is used to determine whether a privacy impact assessment (PIA) is required.

3.69 Where the PTA shows that a project will involve a significant change to DHS's management of personal information or if it might have a significant impact on the privacy of individuals,

then a PIA is required, unless otherwise authorised by the Secretary or a Deputy Secretary. DHS will often use a third party to conduct a PIA.

3.70 The Programme Advice and Privacy Branch has created information and guidance for staff on how to undertake a PTA, which is available to staff on the intranet. They can also provide support and assistance to complete the PTA if required.

3.71 A PIA was not conducted for the PAYG program before it commenced in 2004, prior to the introduction of the OCI (now EIC) system in 2016, or before the changes to introduce the EIC in February 2017. However, during fieldwork, DHS noted that a PTA had been completed in relation to the anticipated changes to the PAYG program that were scheduled to occur after the OAIC's assessment.

Program protocol

3.72 DHS voluntarily adopts the OAIC's Data Matching Guidelines, which, amongst other requirements, specify that agencies should prepare a program protocol to inform the public about the data matching program. A copy of this program protocol should be provided to the OAIC and made publicly available. Topics to be covered by the protocol are set out in Appendix A of the Data Matching Guidelines.

3.73 DHS created a program protocol for the PAYG program when the program formally commenced in 2004. An updated version of the protocol was published in May 2017, following consultation with the OAIC.[27] DHS advised that a review of the protocol must occur every three years. The scope of this assessment did not specifically include examination of the program protocol. However, this assessment presented an opportunity for the OAIC to gain a clearer understanding of the context and technical details of the PAYG program, as well as to discuss the changes to the PAYG program since the publication of the May 2017 version of the protocol.

3.74 The program protocol currently addresses many of the requirements in Appendix A of the Data Matching Guidelines, such as providing an overview of the program, outlining its objectives, and discussing the reasons for conducting the program. However, some sections of the protocol lack sufficient details to provide transparency about how the PAYG program operates. In particular, the OAIC noted the lack of detail in the technical standards report,[28] which DHS included as Appendix A in the May 2017 version of the PAYG program protocol.

3.75 The technical standards report provides very little detail about the matching algorithm used in the program, as well as only a brief overview of the risks associated with the program, the data quality controls employed, and the security and confidentiality safeguards in place to minimise access to personal information.

3.76 Further, some sections of the protocol appeared out-of-date, such as the sample initial contact letter provided at Appendix B of the protocol.

---

[27] All DHS data matching protocols can be viewed on the DHS website at https://www.humanservices.gov.au/organisations/about-us/publications-and-resources/centrelink-program-data-matching-activities.

[28] The requirement for a technical standards report is set out in Guideline 4 of the Data Matching Guidelines, with further detail about the contents of the report set out in Appendix B of the Data Matching Guidelines.

Analysis

PTAs and PIAs

3.77 DHS noted that the data matching process involved in the PAYG program is largely unchanged since the commencement of the program in 2004, and that the program currently uses the same algorithm as it did before the roll out of the automated EIC process. Given that no PTAs or PIAs have been conducted in relation to the PAYG program, except for the PTA conducted in anticipation of the change to the EIC process scheduled for February 2018, many aspects of the PAYG program have not been assessed for potential privacy impacts.

3.78 In addition, there appeared to be a lack of understanding amongst DHS staff during fieldwork that personal information quality is a privacy issue, which was also reflected in discussions about privacy training (see above at paragraph 3.34). Furthermore, personal information quality is not specifically identified as a possible privacy risk area on DHS's PTA form. As a result, there is a risk that even when PTAs and PIAs are being conducted, the risks that poor personal information quality poses, to both a program and customers, may not be included in the PTA or PIA process, and therefore mitigation strategies may not be developed to address any such risks.

3.79 The OAIC understands that, at the time of the assessment, most of the PAYG program compliance process ultimately involved a degree of manual intervention by a DHS compliance officer. Interviews with staff indicated that DHS is aiming to increase the number of customers who complete the entire compliance process online, which will require changes to the current process for identifying customers for whom an online-only process is suitable, as well as changes to communication to customers in letters and the online portal.

3.80 An increase in online-only compliance processes means an increase in automated decision-making without human intervention. Therefore, any changes to the EIC process, especially any that will facilitate automated decision-making, should be preceded by a PTA and/or PIA to evaluate and if necessary, mitigate, any privacy risks to customers. In particular, any PTA/PIA should consider the risks that any change may pose for collecting and using accurate, up-to-date and complete information in the context of automated decision-making.

3.81 The OAIC recommends that DHS continue to conduct PTAs and where appropriate, PIAs for any future changes to the PAYG program, including assessments of personal information quality risks where relevant. DHS should consider including specific questions about personal information quality in its PTA form to raise awareness of the possible privacy implications of poor quality personal information, and ensuring personal information quality is also captured by the PIA process.[29] DHS should also monitor the implementation of any recommendations that arise from such assessments.

Program protocol

3.82 The current version of the program protocol could be improved to enhance transparency

[29] For more information about what to consider from a data quality perspective during the PIA process, see the OAIC's Guide to undertaking privacy impact assessments, and in particular, the section on APP 10 and the 'information quality' heading in the section on mapping information flows.

surrounding the data matching program, and particularly to provide a clearer understanding of how the matched data is handled once it is collected from the ATO. This could include clearly setting out in the 'Action resulting from the program' section details about the automated decision making and manual intervention process that constitutes the EIC system. DHS could also consider providing additional details in the sections on costs/benefit analysis, alternative methods considered, risks, controls and security features. Should any of these details be considered sensitive in nature, the OAIC suggests that DHS create an internal version to outline the technical aspects of the program, such as business rules and filtering. This version could then be used for transparency, auditing, monitoring and quality control purposes.

3.83 The OAIC also suggests that DHS schedule regular reviews of the program protocol to ensure it remains comprehensive and up-to-date. This could be done annually, and after any major change to the PAYG program or relevant legislation, for best privacy practice.

Ongoing reviews

3.84 While consideration of DHS's privacy policy and collections notices is outside of the scope of this assessment, discussions during fieldwork highlighted that the PAYG program has undergone, and will continue to undergo, changes to its scope and how it engages with customers. As a result, the OAIC suggests that any such changes should prompt ongoing reviews of DHS's privacy policy and PAYG program collection notices, to ensure these documents remain as accurate and up-to-date as possible. This can help improve transparency and ensure privacy is routinely taken into account as the PAYG program evolves.

Recommendation 5

The OAIC recommends that DHS:

- continues to conduct PTAs, and where appropriate, PIAs, for any future changes to the PAYG program
- considers including specific questions about personal information quality as part of its PTA form to raise awareness of the possible privacy implications of poor quality personal information, and ensuring personal information quality is also captured by the PIA process
- monitors the implementation of any recommendations that arise out of such assessments.

Part 4: Recommendations and responses

Recommendation 1

OAIC recommendation

4.1 The OAIC recommends that DHS implements additional measures to ensure the personal information it receives from the ATO for the PAYG program is accurate, up-to-date and complete, having regard to the purposes for which the personal information is being used. Such measures could include entering into a more formal arrangement, such as a Memorandum of Understanding with the ATO as a way of dealing with the management of personal information, including personal information quality issues that arise specifically under the PAYG program.

Response by DHS to the recommendation

4.2 Agreed. DHS is confident that the personal information it receives from the ATO for the PAYG program meets the OAIC Guidelines on Data Matching in Australian Government Administration. The collection of personal information is outlined in DHS' Data Matching Protocol.

The ATO and DHS have had a Bilateral Management Arrangement in place for sometime. This is reviewed regularly. The department also have in place a Head Agreement (in place since 2012); the Service Schedule (in place since 2014) and the abridged arrangement for Transfer of Information between ATO and DHS in place since 11 October 2017 and currently under active review.

Recommendation 2

OAIC recommendation

4.3 The OAIC recommends that DHS addresses the quality of the personal information that it uses in its PAYG program by:

- reviewing, and if necessary, improving the data validation techniques it employs at the point of data entry, i.e. when DHS staff enter a customer's personal information into DHS systems
- implementing a regular audit or quality assurance program to examine customer records used in the PAYG data matching program to ensure the information in those records is complete, accurate and up-to-date
- reviewing its staff training to ensure it addresses personal information quality issues and to ensure personal information quality is understood by staff to be a privacy issue.

Response by DHS to the recommendation

4.4 Agreed. DHS recognises the importance of quality assurance of the personal information it uses in the PAYG program, and advises we have already implemented each of the processes recommended by the OAIC.

Recommendation 3

OAIC recommendation

4.5 The OAIC recommends that DHS:

- implements additional measures to facilitate customer-initiated correction of information under the EIC process to ensure the outcome of the EIC process, following review by customers, is that any debt calculation is based on accurate, up-to-date and complete information
- makes all automated and manual compliance intervention processes as easy as possible for customers to understand and use. The EIC process should clearly communicate to customers what information they are being asked to review and how to obtain the correct information to input into the system if required.

Response by DHS to the recommendation

4.6 Agreed. Customers are given several opportunities to correct their records and provide information to DHS prior to a debt being calculated.

Recommendation 4

OAIC recommendation

4.7 The OAIC recommends that DHS implements measures to ensure it is adhering to the minimum procedural requirements in relation to correcting personal information contained in APP 13 (specifically 13.2-13.5), whenever a customer raises concerns about their personal information being incorrect, including during the EIC compliance intervention process.

Response by DHS to the recommendation

4.8 Agreed. The Department complies with the minimum procedural requirements in relation to correction of personal information contained in APP 13. The business area confirms in writing any re-assessment derived from customers' seeking correction of their records.

Recommendation 5

OAIC recommendation

4.9 The OAIC recommends that DHS:

- continues to conduct PTAs, and where appropriate, PIAs, for any future changes to the PAYG program
- considers including specific questions about personal information quality as part of its PTA form to raise awareness of the possible privacy implications of poor quality personal information, and ensuring personal information quality is also captured by the PIA process
- monitors the implementation of any recommendations that arise out of such assessments.

Response by DHS to the recommendation

4.10 Agreed. The Department's Operational Privacy Policy requires that a PTA must be completed for all new projects and any other activities which involve changes to the way the department's manages any personal information. This will include any future changes to the PAYG programme. The Department ensures that all PIAs address all of the APPs in relation to the project, including personal information quality under APP 10. The Department is currently reviewing its PTA form and developing monitoring processes for PIA recommendations and undertakes to apply this recommendation.

Part 5: Description of assessment

Objective and scope of the assessment

5.1 This assessment was conducted under s 33 C(1)(a) of the Privacy Act, which allows the OAIC to assess whether an entity maintains and handles the personal information it holds in accordance with the APPs.

5.2 The objective of this assessment was to determine whether DHS maintains personal information under the PAYG program, in accordance with its obligations under the Privacy Act.

5.3 The scope of this assessment was limited to considering DHS's handling of personal information against the requirements of APP 10 (quality of personal information) and APP 13 (correction of personal information). Specifically, the assessment examined whether DHS is taking reasonable steps to:

- ensure the quality of personal information used in the PAYG program in accordance with APP 10
- correct the personal information it holds in accordance with APP 13.

This assessment did not consider the information handling practices of ATO, which works with DHS on the PAYG data matching program.

Privacy risks

5.4 Where the OAIC identified privacy risks and considered those risks to be high or medium risks, according to OAIC guidance (as set out in Appendix A), the OAIC made recommendations to DHS about how to address those risks. These recommendations are set out in Part 4 of this report.

5.5 The OAIC assessments are conducted as a 'point in time' assessment; that is, our observations and opinion are only applicable to the time period in which the assessment was undertaken.

5.6 For more information about privacy risk ratings, refer to the OAIC's 'Risk based assessments – privacy risk guidance'. Further detail on this approach is provided in Chapter 7 of the OAIC's Guide to privacy regulatory action.

Timing, location and assessment techniques

5.7 The OAIC conducted a risk-based assessment of DHS's PAYG program and focussed on identifying privacy risks to the effective handling of personal information, in accordance with privacy legislation.

5.8 The assessment involved the following:

- review of relevant policies and procedures provided by DHS
- fieldwork, which included interviewing key members of staff and reviewing further documentation at the DHS office in Canberra on 12 and 13 December 2017.

Reporting

5.9 The OAIC publishes final assessment reports in full, or in an abridged version, on its website. All or part of an assessment report may be withheld from publication due to statutory secrecy provisions, privacy, confidentiality, security or privilege. This report has been published in full.

Appendix A: Privacy risk guidance

Privacy risk rating	Entity action required	Likely outcome if risk is not addressed
High risk Entity must, as a high priority, take steps to address mandatory requirements of Privacy legislation	**Immediate management attention is required.** This is an internal control or risk management issue that if not mitigated is likely to lead to the following effects	• Likely breach of relevant legislative obligations (for example, APP, TFN, Credit) or not likely to meet significant requirements of a specific obligation (for example, an enforceable undertaking) • Likely adverse or negative impact upon the handling of individuals' personal information • Likely violation of entity policies or procedures • Likely reputational damage to the entity, such as negative publicity in national or international media. • Likely adverse regulatory impact, such as Commissioner Initiated Investigation (CII), enforceable undertakings, material fines • Likely ministerial involvement or censure (for agencies)
Medium risk Entity should, as a medium priority, take steps to address Office expectations around requirements of Privacy legislation	**Timely management attention is expected.** This is an internal control or risk management issue that may lead to the following effects	• Possible breach of relevant legislative obligations (for example, APP, TFN, Credit) or meets some (but not all) requirements of a specific obligation • Possible adverse or negative impact upon the handling of individuals' personal information • Possible violation of entity policies or procedures • Possible reputational damage to the entity, such as negative publicity in local or regional media. • Possible adverse regulatory impacts, such as Commissioner Initiated Investigation (CII), public sanctions (CII report) or follow up assessment activities. • Possible ministerial involvement or censure (for agencies)
Low risk Entity could, as a lower priority than for high and medium risks, take steps to better address compliance with requirements of Privacy legislation	**Management attention is suggested.** This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the entity or process being assessed.	• Risks are limited, and may be within acceptable entity risk tolerance levels • Unlikely to breach relevant legislative obligations (for example, APP, TFN, Credit) • Minimum compliance obligations are being met