Australian Government

Office of the Australian Information Commissioner

October 2016

Assessment of Schedule 5 of the Foreign Fighters Act

Department of Immigration and Border Protection

Assessment report

Assessment undertaken: February/March 2016

Draft report issued: June 2016

Final report issued: October 2016

www.oaic.gov.au

Contents

Part 1: Executive summary

1.1 This report outlines the findings of the Office of the Australian Information Commissioner's (OAIC) privacy assessment of the Department of Immigration and Border Protection's (DIBP) handling of personal information under Schedule 5 of the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* (Foreign Fighters Act). Schedule 5 of the Foreign Fighters Act expanded DIBP's powers to collect and use personal information from Australian citizens crossing Australia's border.

1.2 The purpose of this assessment was to consider whether DIBP is handling personal information throughout the arrivals and departures border clearance processes in accordance with the Australian Privacy Principles (APPs), and where appropriate, make recommendations to assist DIBP to do so.

1.3 OAIC assessors examined DIBP's relevant internal policies and procedures and conducted interviews with staff in relation to the new powers to collect and use personal information in the context of the border crossing processes. The assessors also received advice on aspects of DIBP's broader information handling practices that support the exercise of these new powers. Where relevant, this advice is noted in this report. However, practices other than those specifically relating to the exercise of powers under Schedule 5 of the Foreign Fighters Act were not considered in detail or in relation to making recommendations.

1.4 The fieldwork component of the assessment was conducted at Brisbane Airport and DIBP's offices in Canberra. The assessors inspected or made enquiries about the operations of key areas involved in border clearance processes, including conducting interviews with Australian Border Force (ABF) officers at Brisbane Airport and DIBP's technical and policy staff in Canberra.

1.5 The OAIC identified medium privacy risks with DIBP's personal information handling practices relating to Schedule 5 of the Foreign Fighters Act. The OAIC has made six recommendations to address those risks.

1.6 The first recommendation (see 4.20) relates to the privacy risk that arises from DIBP needing to have an appropriate level of governance and accountability for the oversight of the exercise of the powers afforded by Schedule 5 during border clearance processes. APP 1.2 requires DIBP to take reasonable steps to implement practices, procedures and systems to ensure it complies with the APPs. The assessors consider that an absence of appropriate practices, procedures and systems, supported by adequate documentation, is not only a risk of breaching APP 1.2, but has the potential to lead to breaches of other APPs.

1.7 The second recommendation (see 6.20) addresses the need for DIBP to enhance the notice it provides to Australian citizens during airport border clearance processes.

1.8 The third recommendation (see 8.24) addresses the need to update or create documentation that supports DIBP's information handling and information security practices in relation to personal information collected during border clearance processes under Schedule 5 of the Foreign Fighters Act, in accordance with APP 11.

1.9 The fourth recommendation (see 8.37) addresses the need for DIBP to review its policies, procedures and systems in relation to the ICT security of personal information collected during border clearance processes.

1.10 The fifth recommendation (see 8.51) addresses the need for DIBP to review its policies, procedures and systems in relation to third party providers supporting the automated border clearance process.

1.11 The sixth recommendation (see 8.62) addresses DIBP's need to enhance the physical security of the layout surrounding the departures SmartGates desk area at Brisbane Airport in order to minimise the risk of misuse, interference, loss and unauthorised access, modification or disclosure of personal information, in accordance with APP 11.

Part 2: Description of assessment

Background

2.1 The Foreign Fighters Act amended the *Migration Act 1958* (Migration Act) and other legislation to introduce a range of measures designed to strengthen and improve Australia's counter-terrorism legislative framework. The amendments commenced on 4 November 2014.

2.2 In its advisory report of October 2014, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommended that the Privacy Commissioner undertake a privacy assessment of the data collected and stored by DIBP whilst exercising powers under the Foreign Fighters Act. It particularly asked the Privacy Commissioner to consider the collection, storage, sharing and use of that data.

2.3 The assessment was conducted under s 33C(1)(a) of the *Privacy Act 1988* (Cth) (the Privacy Act), which allows the OAIC to assess whether personal information held by an APP entity is being maintained and handled in accordance with the APPs.

2.4 Prior to exercising its powers under Schedule 5 of the Foreign Fighters Act through the implementation of departures SmartGates, DIBP completed a privacy impact assessment (PIA) in relation to this process. The PIA provides an overview of the collection of passport scans and facial images by arrivals and departures SmartGates, including the retention of these images and scans. The PIA was provided to the OAIC in draft form for comment in May 2015. The PIA was finalised on 17 June 2015.

Objective and scope

2.5 The objective of this assessment was to establish whether DIBP is handling personal information during border clearance processes in accordance with the APPs while exercising its new powers under Schedule 5 of the Foreign Fighters Act.

2.6 The assessment of the border clearance processes focused on the handling of personal information in accordance with selected APPs. These APPs were APP 1 (open and transparent management of personal information), APP 3 (collection of personal information), APP 5 (notification of the collection of personal information), APP 6 (use or disclosure of personal information) and APP 11 (security of personal information).

2.7 The OAIC assessed the incoming (arrivals) and outgoing (departures) border clearance processes. Within each of these two processes, the OAIC assessed the way in which DIBP handles personal information from the point at which that personal information is collected from Australian citizens during the border clearance process to the point at which that personal information comes to be held in DIBP's databases.

2.8 The scope of this assessment did not include identity verification during border clearance processes for non-Australian citizens. The new powers under Schedule 5 of the Foreign Fighters Act did not alter border clearance processes for non-Australian citizens.

2.9 Identity verification that is separate or supplementary to border clearance processes were outside the scope of this assessment (for example, in relation to visa applications for non-citizens, or where citizens or non-citizens undergo further identity verification after failing to clear the manual or automated border clearance processes).

2.10 The scope of this assessment also did not include the new powers afforded to DIBP under the *Migration Amendment (Strengthening Biometrics Integrity) Act 2015* (refer to 3.6).

Timing, location and assessment techniques

2.11 The assessors conducted the fieldwork component of the assessment on:

- 29 February 2016 at Brisbane Airport, Queensland
- 1 March 2016 at DIBP's offices in Civic and Belconnen, Australian Capital Territory.

2.12 During the fieldwork, the assessors undertook a site inspection of DIBP's facilities relevant to the handling of personal information during border clearance processes at Brisbane Airport and at the National Offices in Canberra. The inspection included an end to end walkthrough of the arrivals and departures border clearance processes at the international terminal of Brisbane Airport.

2.13 The fieldwork also involved semi-structured interviews with key staff to assess DIBP's arrangements for handling personal information during border clearance processes.

2.14 A semi-structured interview with DIBP staff unavailable during the fieldwork was conducted via teleconference on 2 March 2016.

2.15 A semi-structured interview to clarify a small number of factual matters with DIBP staff was also conducted via teleconference on 25 July 2016.

Information obtained during the assessment

2.16 DIBP provided a range of documents before, during, and after the fieldwork relating to its arrangements for handling personal information during border clearance processes. These documents are listed at Appendix A.

Privacy Risks

2.17 The OAIC makes recommendations to address 'high' and 'medium' privacy risks. For more information about these privacy risk ratings, see the OAIC's 'Privacy risk guidance' at Appendix B. Further detail on this approach can be found in Chapter 7 of the OAIC's *Guide to privacy regulatory action*.

2.18 The assessors have made six recommendations to address medium privacy risks identified during the course of this assessment. A recommendation is a suggested course of action or a control measure that, if put in place by DIBP, will (in the opinion of the OAIC) minimise the privacy risks identified around how personal information is handled during border clearance processes.

Reporting

2.19 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.

2.20 This report has been published in full.

Part 3: Assessment context

Schedule 5 of the Foreign Fighters Act

3.1 Schedule 5 of the Foreign Fighters Act amended provisions in the Migration Act (including ss 166, 170 and 175) that applied to the process of crossing Australia's border. The main impacts of the amendments were:

- particular personal identifiers[1] (specifically, an image of a person's face and shoulders — referred to in this report as 'facial images') could be collected by DIBP from Australian citizens who enter or depart Australia. Previously, personal identifiers could only be obtained from non-Australian citizens at the border crossing
- automated border processing control systems, such as SmartGates or eGates (referred to jointly in this report as 'SmartGates'), were authorised to collect these personal identifiers from any person that uses them
- if a person presents a document such as a passport to a clearance authority in person, or to an automated border processing control system, information could be collected by DIBP from that document.

3.2 The purposes for which the personal identifiers collected by DIBP could be used and disclosed were expanded by Schedule 5 of the Foreign Fighters Act through amendments to ss 336D and 336E of the Migration Act to include identifying persons who are a security concern to Australia or a foreign country.

3.3 The assessors focussed on the powers introduced by Schedule 5 of the Foreign Fighters Act in this assessment. The decision to focus on the new powers was informed by issues raised in the PJCIS report on the Foreign Fighters Bill, including the sensitive nature of information proposed to be collected and handled by DIBP (i.e. biometric information). This also enabled the OAIC to gain an understanding of the new processes, and any privacy risks that may arise from those processes, as DIBP handles and secures biometric information collected during the border clearance process into their existing databases.

3.4 However, the assessors also received advice from DIBP on information security arrangements that support the exercise of powers under Schedule 5 during the border clearance processes. This report makes comment on those supporting processes and infrastructure insofar as it is relevant to the exercise of Schedule 5 powers, particularly in relation to information security (refer to Part 8).

3.5 In light of this additional advice, the OAIC intends to undertake a secondary assessment of the security of DIBP's systems that support the border clearance processes, and DIBP's use of the personal information collected by those process in the 2016/17 financial year.

[1] 'Personal identifier' is defined in s 5A of the Migration Act. An image of a person's face and shoulders is 'sensitive information' for the purposes of the Privacy Act (as defined in s 6).

Strengthening Biometrics Act

3.6 The *Migration Amendment (Strengthening Biometrics Integrity) Act 2015* (Strengthening Biometrics Act) commenced on 16 February 2016, and was in effect at the time this assessment was conducted.

3.7 Schedule 1 of the Strengthening Biometrics Act made several amendments to the Migration Act. Provisions in the Migration Act that permitted DIBP to collect personal identifiers, such as ss 166, 170 and 175 as amended by Schedule 5 of the Foreign Fighters Act, were consolidated into a new s 257A. The new s 257A additionally provided DIBP with the discretion to collect further personal identifiers during the border crossing process, such as fingerprint and iris scans.

3.8 The scope of this assessment was limited to DIBP's exercise of its powers under Schedule 5 of the Foreign Fighters Act and did not consider identifiers such as fingerprint and iris scans. These may be the subject of future assessments.

DIBP's organisational structure

3.9 On 1 July 2015 the border control functions of DIBP and the Australian Customs and Border Protection Service (ACBPS) were merged into a single, integrated border agency that retained the title of the Department of Immigration and Border Protection.

3.10 This merger also resulted in the creation of ABF. ABF is a front-line operational branch within DIBP that is responsible for operational border control, investigations, compliance, detention and enforcement functions. DIBP remains responsible for policy, regulatory and corporate activities.

3.11 The transfer of management and responsibility for matters relating to the border clearance, such as automated border clearance processes, from ACBPS to DIBP and ABF was ongoing at the time of this assessment.

Overview of border clearance processes

3.12 Border clearance processes described in this report are particular to the assessors' observations at Brisbane Airport.

Arrivals

3.13 Australian citizens (citizens) arriving in Australia proceed to the arrivals hall after disembarking from their flight. All citizens must complete an Incoming Passenger Card (IPC). IPCs are available at a counter located ahead of the arrivals hall.

3.14 All citizens have their identity verified in the arrivals hall in order to cross the border. Citizens can choose to have their identity verified manually by an ABF officer, or, if they have an ePassport,[2] can choose to have their identity verified through the automated SmartGate process.

[2] ePassports have an embedded microchip which contains the same personal information that is on the color photo page of the passport, including a digitised photograph.

Manual border clearance process

3.15 Citizens who choose to have their identity verified through the manual process produce their passport to an ABF officer sitting at a counter, who scans it. In this scan, information including the passport photo is collected and transferred to DIBP databases, where it is retained indefinitely.

3.16 The ABF officer compares the photo on the passport with the citizen's appearance in person. The citizen is then either cleared to cross the border, or if necessary, is subject to additional identity verification.

Automated border clearance process

3.17 Citizens who choose to have their identity verified through the arrivals SmartGate process first go to a computer kiosk, and insert their passport open at the photo page into a slot in the kiosk. The kiosk scans the passport and collects data from it, including biographical information, a scan of the passport photo and photo data stored in the passport's electronic chip.

3.18 After the passport scan, the kiosk prompts the citizen to review an electronic privacy notice. The citizen must press the computer screen to acknowledge the notice. The kiosk then generates a ticket for the citizen to collect and feed into the SmartGate. The ticket contains the data collected by the kiosk in a format that can be read by the SmartGate.

3.19 After the SmartGate reads the ticket to recall the information collected at the kiosk, the citizen is directed to look at a camera positioned inside the SmartGate. The camera captures a facial image of the citizen. The SmartGate then generates a biometric template from the image captured by the camera. This template is compared against a second biometric template generated from the image captured at the kiosk.

3.20 The SmartGate uses an algorithm to verify the citizen's identity by calculating the compatibility of the two biometric templates that have been generated. If the biometric templates are matched above a pre-determined threshold, the SmartGate will allow the citizen to proceed. If the biometric templates do not match above this threshold, the citizen is directed to the manual border clearance process by moving back out of the SmartGate.

3.21 After the citizen has passed through the SmartGate, the scanned passport photo and the facial image of the citizen taken by the SmartGate camera are both transferred to the same DIBP information database that holds passport photo scans collected during the manual arrivals process. The biometric templates are not retained beyond the border clearance process.

3.22 In both the manual and SmartGate processes, the citizen retains the IPC so that it can be surrendered to an ABF officer at a subsequent checkpoint.

Departures

3.23 Australian citizens seeking to depart from Australia proceed to the departures hall in the airport. All citizens are required to complete an Outgoing Passenger Card (OPC). OPCs are available at a counter located ahead of the entry to the departures hall.

3.24 All citizens have their identity verified in the departures hall in order to cross the border. Citizens can choose to have their identity verified manually by DIBP staff or through the automated SmartGate process, which accepts all passports.

Manual border clearance process

3.25 The manual border clearance process for departing citizens is the same as the process described above for arriving citizens, with the exception that information collected in the arrivals and departures processes is stored in separate DIBP databases.

Automated border clearance process

3.26 Citizens that choose to have their identity verified through the SmartGate process go to the SmartGate and place their passport onto a passport reader. Importantly, citizens are not required to attend a kiosk prior to entering the departures SmartGate. Instead, a reader inside the SmartGate scans the passport photo and generates a biometric template from this photo.

3.27 The citizen is directed to look at a camera positioned inside the SmartGate. The camera captures a facial image of the citizen. The SmartGate then generates a biometric template from the image captured by the camera.

3.28 The SmartGate uses an algorithm to verify the citizen's identity by calculating the compatibility of the two biometric templates that have been generated. If the biometric templates are matched above a pre-determined threshold, the SmartGate will allow the citizen to proceed. If the biometric templates do not match above this threshold, the citizen is directed to the manual border clearance process.

3.29 After the citizen has passed through the SmartGate (including if the citizen is subsequently directed to the manual border clearance process), the scanned passport image and the facial image captured by the SmartGate camera are both transferred to the same DIBP information database that holds passport photo scans collected during the manual departures process. This database is different to the database in which images collected during the arrivals SmartGate process are stored. The biometric templates are not retained beyond the border clearance process.

3.30 In both the manual and SmartGate processes, once the citizen has cleared the border they place their OPC inside a box that is positioned behind the ABF counters and SmartGates. OPCs contained in the box are periodically removed by an ABF officer and bundled together with other, previously collected OPCs, before being sent by courier to a service provider to electronically scan the cards.

Part 4: Assessment issues — Open and transparent management of personal information

4.1 Under APP 1.2(a) an APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that will ensure it complies with the APPs. Under APPs 1.3-1.6 an APP entity must have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information and makes the policy available.

Observations on privacy policy

4.2 The assessors reviewed DIBP's privacy policy, which is available on DIBP's website free of charge, prior to undertaking the fieldwork activities. The assessors note that although SmartGates are not mentioned in any detail, the privacy policy outlines DIBP's authority to collect, use and disclose personal information under authorising legislation. The assessors took the view that DIBP's privacy policy covers the information required under APP 1.4(a) to (g).

4.3 The assessors noted that Part D of the privacy policy provides a hyperlinked reference to additional information on SmartGates. The majority of the information contained on the hyperlinked page was relevant only to arrivals SmartGates. The OAIC suggests that DIBP revises the information on this page to take account of departures SmartGates.

Observations on practices, procedures and systems

4.4 Overall, the assessors observed a lack of clear responsibility for the oversight and ongoing management at DIBP of practices, procedures and systems for handling personal information during border clearance processes in accordance with the powers afforded by Schedule 5.

4.5 The assessors noted that the DIBP teams interviewed in the course of this assessment had distinct responsibilities in relation to border clearance processes. Within their areas of responsibility, the assessors noted that DIBP staff are aware of their specific operational requirements. However, it was unclear to the assessors whether DIBP staff are aware of the privacy implications associated with Schedule 5 and automated border clearance processes, especially at a level beyond their own team's operational requirements.

4.6 During interviews with DIBP staff in Canberra, the assessors were advised that responsibility for the oversight of technical aspects and policy arrangements of the arrivals and departures SmartGates are separated across different teams within DIBP.

4.7 The assessors understand that, prior to the merger of ACBPS and DIBP on 1 July 2015, ACBPS was solely responsible for practices, procedures and systems relating to the automated border clearance processes, including in relation to Schedule 5. Post-merger, this responsibility has been split across different DIBP teams.

4.8 The Future Traveller Capability Taskforce within DIBP is currently responsible for the technical development and implementation of SmartGates. This taskforce includes two separate teams that are independently responsible for arrivals and departures SmartGates.

4.9 A separate team within DIBP is currently responsible for policy matters relating to SmartGates, having assumed responsibility for this on 1 July 2015. Prior to the merger this DIBP policy team developed policies for DIBP's collection of biometric information to the exclusion of automated border clearance processes, as this was ACBPS's responsibility.

4.10 The ACBPS privacy and legal team which was engaged with the team responsible for the technical development of SmartGates, and provided advice on privacy matters associated with those SmartGates (e.g. the privacy signage discussed in Part 5), was disbanded after the 1 July 2015 merger.

4.11 A Privacy and Reviews team with responsibility for privacy matters within DIBP as a whole had been newly established in the merged DIBP entity at the time of this assessment.

4.12 Finally, the assessors were advised that ABF is responsible for the day-to-day operational control of the SmartGates. At the time of this assessment, ABF officers were also responsible for the training of officers using SmartGates.

4.13 During interviews with the teams described above, the assessors observed inconsistencies in the understanding amongst the members of each of these teams on how personal information is handled during border clearance processes. In particular, the assessors were provided with inconsistent advice around the period of time DIBP retains personal information collected during border clearance processes.

4.14 The assessors also observed that critical sections within DIBP were unaware of certain policy documents relating to Schedule 5, such as the PIA noted at paragraph 2.4 above. The assessors understand that the PIA had not been circulated amongst DIBP staff at the time of this assessment.

Privacy issues in relation to practices, procedures and systems

4.15 The assessors consider that the absence of clear responsibility for the ongoing management and privacy oversight of border clearance processes is a medium privacy risk of DIBP not having taken reasonable steps to implement practices, procedures and systems to ensure it complies with the APPs, as required by APP 1.2.

4.16 The assessors understand that this may be in some respects attributable to the recent merger of DIBP and ABCPS. The assessors considered that there appeared to be a loss of corporate knowledge in relation to privacy matters associated with border clearance processes after the disbandment of the ACBPS team that was responsible for those matters.

4.17 The assessors note that the Privacy and Reviews team now has responsibility for responding to privacy issues relating to border clearance processes. However, the assessors were also informed that this section had not been provided with key information relating to Schedule 5, such as the Schedule 5 PIA. The assessors considered that this may have impacted the broader understanding and communication of privacy risks relating to the management of new powers afforded under Schedule 5 throughout DIBP.

4.18 In the assessors' opinion, there is a need for clear responsibility for the ongoing privacy management of border clearance processes, which is a currently medium risk of non-compliance with APP 1.2, resulting in an inconsistent understanding of information handling practices amongst DIBP staff. This has also impacted upon the management of documentation and DIBP staff training that supports the powers afforded by Schedule 5. Issues surrounding DIBP documentation and training are discussed further at 8.8-8.23.

4.19 This also leads to risks of breaching other APPs, in particular APP 11 which is discussed further in Part 8.

Recommendation 1

4.20 The assessors recommend that DIBP introduces governance measures to ensure an appropriate level of responsibility and accountability for the oversight and implementation of practices, procedures and systems for handling personal information during border clearance processes in accordance with Schedule 5 of the Foreign Fighters Act.

Part 5: Assessment issues — Collection of solicited personal information

5.1 Under APP 3, an APP entity may only collect solicited personal information (other than sensitive information) where it is reasonably necessary for, or directly related to, an agency's functions or activities.

5.2 For most APP entities, APP 3 additionally requires the individual concerned to provide consent if sensitive information is being collected from them. However, as DIBP is listed as an enforcement agency in the Privacy Act, it is excepted from this requirement under APP 3.4(d)(i), provided that the collection of information is reasonably necessary for, or directly related to, one or more of its enforcement related activities.

5.3 DIBP collects personal information from all persons that cross the border. Depending on the process an Australian citizen follows to cross the border (as described at 3.12-3.30), DIBP will collect, at a minimum, information contained on that citizen's passport, including the passport photo, and information written on an IPC or OPC.

5.4 For citizens that use an automated border clearance process, DIBP will additionally collect a facial image. Under the Privacy Act, biometric information that is to be used for the purpose of automated biometric verification or biometric identification is sensitive information. As such, facial images, when used through the SmartGates, are considered to be sensitive information.

5.5 DIBP advised that the primary purpose for the collection of a facial image during the border clearance process is to identify individuals at the border and validate travel documents for border clearance and control.

5.6 The assessors consider that the collection of passport information, information written on IPCs and OPCs, and facial images is directly related to DIBP's border clearance processing functions. The assessors did not identify any issues in relation to the collection of personal information in this assessment.

Part 6: Assessment issues — Notification of the collection of personal information

6.1 APP 5 relates to collection notices. An APP entity that collects personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters.

6.2 An APP entity must take these reasonable steps before or at the time it collects personal information. If this is not practicable, reasonable steps must be taken as soon as practicable after collection.

Observations on notification of the collection of personal information

Arrivals

6.3 The assessors noted that IPCs refer citizens to a *Form 1442i* privacy notice available on DIBP's website. The assessors considered that *Form 1442i* contains the matters required for a notice under APP 5.2, in the context of Schedule 5.

6.4 The assessors observed that citizens who elect to use the arrivals SmartGates are also presented with an electronic privacy statement at the computer kiosk before they enter the SmartGate. A citizen must touch the screen to acknowledge the privacy statement in order to proceed from the kiosk to the SmartGate.

6.5 DIBP staff advised, however, that citizens who elect to proceed through a manual border clearance process will not receive an equivalent privacy statement during that manual process to the one provided by the kiosk.

Departures

6.6 The assessors noted that OPCs also refer citizens to a *Form 1442i* privacy notice available on DIBP's website.

6.7 Departures SmartGates do not operate using a kiosk system. As a result, the opportunity to present an electronic privacy statement that travellers must acknowledge (as seen via the arrivals kiosk) is not available in the departures hall. Electronic privacy statements have not been built into the departure SmartGates. The assessors understand that this has been done to reduce time taken for passengers to pass through the border clearance process.

6.8 The assessors observed physical signage displaying privacy notifications in multiple locations throughout the departure process. Firstly, two A4 sized signs displaying a privacy statement were affixed to the wall above the counter outside the departures hall where OPCs were available. Secondly, inside the departures hall five signs of varying sizes displaying a privacy statement were placed at locations visible from the queue for the departures SmartGates.

6.9 The privacy notifications on the signage contained a reference to the web address for DIBP's privacy policy. The largest of these signs was A4 sized. All of the signage was written in English only.

6.10 The assessors also observed several electronic screens visible throughout the departures process. Two screens, which cycled through several different messages, appeared side by side at the entry to the SmartGate queueing area. A further two screens, showing an instructional video demonstrating how to use the SmartGates, appeared side by side immediately above the entry to the SmartGates. No privacy statement, or information relating to the handling of personal information by the SmartGates, was displayed on any of the electronic screens.

6.11 ABF officers also advised that hard copy versions of the privacy statement or any additional privacy documents were not available in the departures hall, and could not be produced on request by ABF officers.

Privacy issues in relation to the notification of the collection of personal information

6.12 The assessors acknowledge the 'layered' approach to privacy notification taken by DIBP. The short statement on privacy on the IPC and OPC refers citizens to the *Form 1442i* privacy notice, and privacy notification signage in the departures hall refers citizens to DIBP's online privacy policy.

6.13 However, in order for notice to be provided to citizens in accordance with APP 5, the first 'layer' of the notifications provided needs to ensure that an individual is aware of the matters referred to in APP 5.2 at or as close as is practicable to the time of collecting their information. In this assessment, the assessors particularly considered the adequacy of the privacy notification signage in the departures border clearance process.

6.14 The assessors consider that the current privacy notification signage in the departure border clearance process, offered as part of that layered approach, raises a medium risk of non-compliance with APP 5. Specifically, several privacy notifications methodologies that were specifically identified by DIBP in its PIA of Schedule 5 (described below) are currently unavailable in the Brisbane Airport departures hall.

6.15 The Revised Explanatory Memorandum for the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* notes at [351] that the departures SmartGates will '…comply with the *Privacy Act 1988*, specifically Australian Privacy Principle 5'.

6.16 The assessors note the advice of DIBP staff that requiring all travellers that pass through the departures hall to acknowledge a privacy statement in a manner consistent with the arrivals SmartGate kiosk (e.g. an electronic privacy statement that passengers must physically acknowledge) would impact on the efficiency and resources involved in the border clearance process.

6.17 However, in lieu of a system comparable to the arrivals process where travellers acknowledge a privacy statement, the Schedule 5 PIA, drafted by DIBP, states:

> Rather than obtaining individual consent from each individual to collect their personal identifiers, information about the collection is made available via prominently placed signs as well as information pamphlets. (p. 16)
>
> The Privacy Statement signage is located on electronic screens on columns and fixed signage on columns where travellers queue for Departures SmartGates. (p. 11)

6.18 Although privacy statement information was made available to citizens on fixed signage in the departures hall, the other notification methods outlined in the PIA (electronic signage and information pamphlets) had not been implemented at the time of this assessment.

6.19 The assessors therefore consider that, in recognition of the sensitivity of the information being collected from citizens during the departures border clearance process, the existing signage may not adequately inform citizens of the handling of their information through the departure SmartGates, and may risk breaching APP 5. The assessors also consider that implementing the additional notification methodologies identified in the Schedule 5 PIA is a reasonable step for DIBP to take in meeting its obligations under APP 5.

Recommendation 2

6.20 The assessors recommend that DIBP enhances its privacy notifications in the departures hall at Brisbane Airport and consider the application of similarly enhanced privacy notifications across all Australian airports.

Additional observation — arrivals hall

6.21 The assessors noted that, in the arrivals hall, the privacy notice that a citizen receives will vary depending on the border clearance process that citizen follows (see 6.3-6.5). Citizens who elect to follow a manual border clearance process will have their passport scanned, including the passport photo, but will not have a facial image captured in accordance with the powers afforded to DIBP under Schedule 5 of the Foreign Fighters Act. As such, notification standards applying to the manual border clearance process in the arrivals hall is technically outside of the scope of this assessment.

6.22 However, in the interests of enhancing privacy notification for travellers electing the manual border clearance process in the arrivals hall, DIBP may consider applying a privacy notification approach that is consistent across the manual and automated border clearance processes.

Part 7: Assessment issues — Use or disclosure of personal information

7.1 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. Information collected by DIBP during border clearance processes that is sensitive information (see 5.4 above) can be used for a secondary purpose if DIBP reasonably believes that it is necessary for the conduct of one or more of its enforcement related activities.

Observations on use or disclosure of personal information

7.2 The assessors understand that the facial images and passport scans collected by SmartGates are used to identify persons who are a security concern to Australia or a foreign country during border clearance processes. DIBP staff also advised that the facial images collected by SmartGates are also occasionally used for testing the automated functionality of the arrivals and departures SmartGates. An example of this is to test the accuracy of the algorithm the SmartGates use to compare biometric templates.

7.3 DIBP staff advised that the facial images and other personal information collected during the border clearance processes can be disclosed to law enforcement and other authorised entities by authorised DIBP staff.

7.4 The process of searching through DIBP databases and accessing the personal information collected during border clearance processes stored in those databases constitutes a use of that information for the purposes of APP 6.

7.5 DIBP staff also advised that the facial images and other personal information collected during the border clearance processes are presently being retained in DIBP's databases with a view to DIBP using this information for other, as yet unspecified, purposes at a later time. The PIA on Schedule 5 notes (on p. 13) 'the capability to retain biometrics for comparison in the future supports detections, investigations, and possible prosecutions of breaches'.

Privacy issues in relation to use or disclosure of personal information

7.6 The uses and disclosures of personal information collected by DIBP during border clearance processes that the assessors considered as part of this assessment were in accordance with the primary purpose for which they were collected, in accordance with Schedule 5 of the Foreign Fighters Act, and are consistent with APP 6.

7.7 The assessors note that the Foreign Fighters Act expanded the purposes for which personal information collected during border clearance processes can be accessed and disclosed. Specifically, that the information can be disclosed to authorised law enforcement bodies to identify a person who may be of national security concern. As such, the disclosure of personal information to law enforcement agencies is consistent with APP 6.

7.8 Whilst the assessors consider that the current use and disclosure of personal information collected by DIBP during border clearance processes is in accordance with APP 6, the assessors

note that the potential future uses of this personal information (as mentioned above at 7.5) will need to be in accordance with APP 6. Specifically, future uses must be in accordance with the primary purpose for which the personal information was originally collected, or an authorised secondary purpose, or permitted as a result of the operation of an exception under APP 6.

7.9 The assessors suggest that before DIBP accesses the information previously collected during border clearance processes for any future uses, DIBP conducts a privacy impact assessment. Further information on conducting privacy impact assessments can be found in the OAIC's *Guide to undertaking privacy impact assessments.* The OAIC may conduct a secondary performance assessment to consider any future uses of the personal information collected by DIBP, and the security arrangements surrounding those uses.

Part 8: Assessment issues — Security of personal information

8.1 Under APP 11, an APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

8.2 The OAIC's *Guide to securing personal information* outlines various operational areas in which entities can take reasonable steps to protect personal information in accordance with APP 11. The assessors considered several of these areas in this assessment as they applied to the exercise of the Schedule 5 powers, including governance, culture and training; internal practices, procedures and systems; ICT security; access security; third party providers; data breaches; physical security; and destruction and de-identification.

8.3 The assessors obtained information from DIBP documents and interviews with DIBP staff in order to consider the areas outlined in 8.2 in the context of the border clearance processes under Schedule 5.

8.4 As noted at 3.5, the OAIC intends to undertake a secondary assessment of the security of DIBP's systems that support the border clearance processes, and the use of these systems by DIBP, in the 2016/17 financial year. Observations on the security of personal information in Part 8 of this report may be the subject of more detailed consideration in that assessment.

Governance, culture and training

8.5 Observations and comments in relation to DIBP's overall governance arrangements for handling personal information during border clearance processes are set out in Part 4 of this report. The following observations and comments focus on governance issues that are specific to the security of personal information.

8.6 The Assessors observed that DIBP staff that work directly with border clearance processes generally have an understanding of the importance of security within the handling of personal information. Discussions on security measures adopted by DIBP staff responsible for the technical design of the departure SmartGates, as well as ABF staff at Brisbane airport responsible for the operations of the SmartGates, confirmed this understanding.

8.7 However, the assessors consider that the governance measures to be introduced in response to Recommendation 1 should include clear procedures for oversight and accountability for decisions regarding personal information security. Without these measures currently in existence, there has been an impact on DIBPs internal practices, procedures and systems, most notably the supporting security documentation and training of staff on privacy matters related to the border clearance processes.

Internal practices, procedures and systems

Observations — Internal practices, procedures and systems

8.8 The assessors examined a number of documents as part of the assessment of DIBP's border clearance processes. The assessors observed that there was no single document available to DIBP

staff or ABF officers that explains the flow of information during border clearance processes, and how this information is protected from interference or misuse.

8.9 The assessors observed conflicting advice within documentation around the retention periods for personal information captured throughout the border clearance processes. DIBP staff also acknowledged an absence of a destruction policy for information collected during border clearance processes.

8.10 Documents outlining aspects of DIBP's information handling and security practices as they relate to the border clearance processes were provided to the assessors. Relevantly, these documents are as follows:

Passengers Enabling Future Traveller System — Biometric Data Retention Policy (SmartGate and Primary Line)

8.11 This document sets out ACBPS's policy on the retention of information captured by SmartGates. This document was last updated on 31 March 2014, and therefore only pertains to arrivals SmartGates. The document states that it is ACBPS policy to retain ePassport Photos and Live Photos (captured by a SmartGate), and Live Biometric Templates (generated by a SmartGate) indefinitely. However, the document later proposes that the retention period for ePassport Photos and Live Photos is amended to 100 years, and that Live Biometric Templates are not retained beyond their initial use.

PAM3: Act — Identity, biometrics and immigration status: Identity information — Access and disclosure

8.12 The stated scope of this manual for DIBP staff is to provide guidance on the provisions in the Migration Act and Privacy Act as they relate to accessing, disclosing, modifying or destroying a person's identity information. The manual notes that it has not been fully reviewed since March 2012. As a result, the manual does not take account of privacy matters related to automated border clearance processes.

Privacy Impact Assessment — Identifying persons in Immigration Clearance — Schedule 5 — Counter Terrorism Legislation Amendment (Foreign Fighters Act) 2014

8.13 The PIA contains some information explaining at a high level the flow of information through border clearance processes and the information security arrangements surrounding information collected by departures SmartGates. However, the PIA has not been made available to DIBP staff or published to the public. The assessors also noted that, in relation to the retention of information collected during border clearance processes, the PIA states that 'ACPBS retains an individual's photograph for a period of 13 years if the individual is processed using a SmartGate' (p. 22).

Instrument of Authorisation 2016/001

8.14 The Instrument of Authorisation 2016/001 outlines the DIBP officers entitled to access personal information collected during border clearance processes for the purpose of disclosing that information to law enforcement agencies (as outlined in Part 7). Whether DIBP maintains a documented process governing the steps DIBP staff were required to follow when disclosing personal information for this purpose was not considered in this assessment, and may be considered as part of a later assessment.

Australian Border Force Departure SmartGates Business Process Training — Facilitator Guide

8.15 The Facilitator Guide provides extensive detail on operational features of the departures SmartGates. However, it does not reference any privacy-related matters for the automated border clearance process.

8.16 The assessors consider that since the training material does not contain any privacy-related material, there is a risk that frontline ABF officers are not appropriately informed about the information flows that occur during border clearance processes. Since frontline ABF officers are in a position to answer questions from citizens about the collection of their personal information, the assessors consider that it is necessary for these officers to be informed about these information flows, or at least able to direct travellers to relevant privacy notifications in accordance with APP 5.

Privacy issues — Internal practices, procedures and systems

8.17 The assessors consider that there is a lack of appropriate documentation to support DIBP's information handling and information security practices in relation to border clearance processes.

8.18 The assessors consider that the absence of documented guidance for DIBP staff on the information flows during border clearance processes, and the appropriate handling of personal information collected as part of these information flows, presents a medium risk of breaching of APP 11.

8.19 Assessors also consider that the content of certain documentation provided to the assessors for examination as part of this assessment, discussed above, does not appear to outline processes to appropriately protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

8.20 In particular, the inconsistent advice in relation to the retention period for information collected during border clearance processes presents a risk that DIBP staff do not understand whether and/or how to de-identify or destroy this information.

8.21 The assessors consider that neither the 'Passengers Enabling Future Traveller System — Biometric Data Retention Policy (SmartGate and Primary Line)' policy document nor the 'PAM3: Act — Identity, biometrics and immigration status: Identity information — Access and disclosure' procedures advice manual are sufficiently up to date to capture current usage of DIBP's border clearance processes, or the handling of personal information throughout those processes.

8.22 The absence of documented policies governing the processes that must be followed when personal information is disclosed, irrespective of whether those disclosures are authorised by law, also presents a risk that personal information could be used or disclosed by DIBP staff in a manner that is not adequately secure.

8.23 Finally, the assessors suggest that incorporating an overview of the flow of information from collection through to retention, and how personal information should be handled during this information flow into the SmartGates Business Process Training may be a means by which DIBP can provide ABF officers with appropriate guidance.

Recommendation 3

8.24 The assessors recommend that DIBP reviews and, where necessary, creates documentation that governs the handling of personal information during border clearance processes in accordance with Schedule 5 of the Foreign Fighters Act. The assessors recommend that the documentation to be reviewed and/or created includes, but is not limited to:

- policies on the destruction or de-identification of information collected during border clearance processes
- training and guidance for DIBP staff and ABF officers on any privacy risks that arise throughout the flow of information collected during border clearance processes and how to mitigate them
- a response plan for incidences of a data breach.

ICT security

Observations — ICT security

8.25 During interviews with DIBP staff, the assessors were provided with an overview of the ICT security arrangements that apply to personal information captured by the arrivals and departures SmartGates.

8.26 The assessors were advised that there are differences between the technical composition of the departures and arrivals SmartGates. A team of staff responsible for technical aspects of the arrivals SmartGates operates independently from an equivalent team responsible for the departures SmartGates.

8.27 Notwithstanding these differences, the assessors understood that there are certain information security arrangements that apply to both the arrivals and departures SmartGates processes. These include:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

8.28 [redacted]

8.29 [redacted]

8.30 The assessors were advised that the ICT systems underpinning SmartGates undergo regular security testing.

8.31 At Brisbane Airport, the assessors observed DIBP's ICT arrangements for maintaining back-ups of information collected during border clearance processes in a server room. [redacted]

Privacy issues — ICT security

8.32 The assessors note that the scope of this assessment did not extend to a detailed examination of all aspects of the ICT systems that relate to the automated border clearance processes, or a

consideration of DIBP's wider ICT systems which interact with the border clearance processes. The OAIC may consider these as part of a future assessment.

8.33 Nevertheless, the assessors consider that the high-level information provided by DIBP in relation to the ICT systems supporting the automated border clearance processes indicate a medium level risk of breaching APP 11.

8.34 [redacted]

8.35 [redacted]

8.36 The OAIC's *Guide to securing personal information* notes that the use of encryption, in combination with other strategies, is important in many circumstances to ensure that information is stored in a form that cannot be easily understood by unauthorised individuals or entities. As noted above (see 5.4), facial images collected via the automated border clearance processes are considered to be sensitive information.

Recommendation 4

8.37 The assessors recommend that DIBP reviews its policies, procedures and systems in relation to the ICT security of personal information collected during border clearance processes, particularly in relation to manual information handling processes and data encryption.

Access security

Observations — Access security

8.38 The assessors observed that access to Brisbane Airport control rooms that monitor the images captured by the SmartGates and server rooms requires the use of an electronic swipe card. Visitors to restricted areas must sign a register of their attendance, and carry a visitor pass. CCTV surveillance cameras are also in operation in the arrival and departure halls, as well as inside the airport restricted areas.

8.39 The assessors also observed the access control arrangements in place for visitors to DIBP's Canberra offices in Civic and Belconnen. At both offices, entry and exit to restricted areas requires the use of an electronic swipe card. All visitors must sign a register of their attendance, and carry a visitor pass.

8.40 The assessors were advised that the level of access provided to DIBP's IT systems, including the IT systems that operate SmartGates, depends on the credentials of the DIBP or ABF officer who logs on to a computer. The assessors noted that the Instrument of Authorisation 2016/001 document specifies the roles of DIBP staff and/or contractors who are entitled to access identifying information collected during border clearance processes.

8.41 ABF officers who are responsible for operating computers as part of the border clearance process, to either control aspects of the SmartGates or to use images captured by SmartGates to perform the manual border clearance process, are required to pass through specific training in order to be authorised to access these computers.

8.42 Access to DIBP's IT systems, servers and databases is logged for auditing purposes. The assessors were advised that DIBP uses passwords and unattended screen lock protection for all computers, including computers operated by ABF officers during border clearance processes. DIBP's

passwords must contain at least 10 characters with a minimum of one upper case letter, one lower case letter and one number.

Privacy issues — Access security

8.43 The assessors did not identify any privacy risks associated with access security as it applied to DIBP's border clearance processes. The assessors noted the advice of DIBP staff about access controls that are applied across DIBP, and these may be considered in greater detail in a future assessment.

Third party providers

Observations — Third Party Providers

8.44 The assessors were advised that DIBP procured the physical departures SmartGates from a third party provider. Another third party provider is responsible for the ongoing maintenance of the biometric algorithm and software used by the departures SmartGates and the servers and databases in which information collected by the SmartGates is stored.

8.45 In relation to the provider responsible for the physical SmartGates, the assessors were advised that the provider has remote access to the SmartGates' operating system for the purposes of monitoring the performance of the SmartGates and fixing any technical issues that arise. This provider does not have access to traveller information captured by the SmartGates.

8.46 In relation to the provider responsible for the biometric algorithm, software, servers, and databases, the assessors were advised that access to the servers and databases that is available to the provider is governed by contractual terms between DIBP and the provider. The assessors were advised that the provider's staff are able to access the personal information stored in these servers and databases, and that the provider's staff would have relevant clearance levels allowing them access to this information. All incidences of access to the servers and databases are logged for auditing purposes. New requests for access to the servers and databases are subject to authorisation by security officers at DIBP and the provider.

Privacy Issues — Third Party Providers

8.47 The assessors note that the scope of this assessment did not extend to a detailed examination of all aspects of the relationship between DIBP and the third party providers that support the border clearance processes. Nevertheless, the assessors consider that the high-level information provided by DIBP in relation to the third party providers that support the border clearance processes indicate a medium level risk of breaching APP 11.

8.48 The OAIC's *Guide to securing personal information* notes that APP entities should consider the scope of personal information handling arrangements with third party providers, and that security and contractual controls should be in place to manage the scope of these arrangements.

8.49 Whilst the staff of the third party provider are subject to a clearance process and logs that are kept of access to DIBP's servers and databases, assessors consider that the maintenance of these servers and databases should not necessitate unrestricted access to the personal information contained in the servers and databases.

8.50 Furthermore, the assessors consider that the importance of DIBP taking steps to limit third party providers' access to personal information is increased by virtue of the sensitivity of the information collected during the border clearance processes, and the absence of encryption as a security measure to protect that information as it sits within DIBP's servers and databases (see 8.32-8.37).

Recommendation 5

8.51 The assessors recommend that DIBP reviews its policies, procedures and systems in relation to the levels of access that are granted to third party providers supporting the automated border clearance process.

Data breaches

8.52 In interviews with ABF officers, the assessors were advised that, as part of compulsory training, all ABF officers are informed that any incidences of a data breach that may occur in relation to border clearance processes are required to be reported to senior ABF staff. The assessors also note that staff in the newly established Privacy and Reviews Team act as DIBP Privacy Contact Officers.

8.53 The assessors were not provided with documentation by DIBP that indicated a formalised response plan for data breaches in relation to border clearance processes. In keeping with the OAIC's *Guide to developing a data breach response plan*, the assessors note that having a response plan is important to mitigate the privacy risks that may follow from any incidences of a data breach. Recommendation 3 addresses this risk.

Physical security

Observations — physical security

8.54 In the departures hall, the assessors observed that behind the departures SmartGates there is a long desk with a row of computers. One computer was manned by an ABF officer who was monitoring a live feed of the images captured by the departures SmartGates, including the passport image scanned by the SmartGate. That ABF officer could control the operation of the gate if necessary.

8.55 Another computer was manned by an ABF officer who was performing the manual border clearance process for travellers who have been referred to them by other ABF officers after failing to clear the SmartGates process. The computer used by that ABF officer displayed travellers' facial images taken from a passport scan and by the SmartGate camera.

8.56 The assessors observed that the desk area occupied by the ABF officers, and the computer screens, was easily visible and accessible to any traveller that walked past the desks. Although there were some barriers in place immediately behind the desk and computers to limit physical intrusion into the area, the barriers were transparent at eye level and did not prevent access to the area from the sides.

8.57 The assessors also observed that, upon passing through the departures SmartGates, travellers placed their OPCs inside a clear box. Because the box was clear, information written on the OPCs could be seen by persons walking through the area. An ABF officer was stationed immediately

behind the departures SmartGates as a security measure to prevent persons from loitering in the area and capturing information contained on the OPCs or displayed on the computers at the desk.

8.58 The arrivals hall does not have an equivalent control desk behind the arrivals SmartGates. Further, ABF officers situated at desks with computers conducting the manual border clearance process were not exposed to public view.

Privacy issues — physical security

8.59 The assessors consider there is a medium risk of breaching APP 11 resulting from the layout of the area in the departures hall manned by ABF officers immediately behind the departures SmartGates. In particular, this risk refers to the visibility of personal information on the computer screens on the desk, and on the OPCs inside the clear box they are deposited in.

8.60 ABF officers were proactive in acknowledging the privacy risks associated with the design of the desk area. ABF officers also advised that the current layout is a temporary arrangement; and that the desk and computers will be relocated and made secure upon the installation of additional SmartGates in the departures hall.

8.61 The assessors note that DIBP has taken steps to mitigate the risk raised by the transparent OPC box by positioning an officer immediately behind the departures SmartGates. ABF officers also advised that at the time of this assessment they had ordered transfers that would be used to cover the surface of the box.

Recommendation 6

8.62 The assessors recommend that DIBP enhances the physical security of the departures SmartGates desk area and the OPC box as necessary to prevent persons being able to view personal information, written or visual.

Destruction and de-identification

Observations — destruction and de-identification

8.63 It was unclear to the assessors whether DIBP has a consistent destruction and/or de-identification policy for personal information collected during border clearance processes. The assessors understand that the present DIBP policy for information collected during border clearance processes is for indefinite retention of this information, although DIBP's documented policies also suggest that this information is to be destroyed either 13 years or 100 years after collection.

8.64 The assessors were advised that the databases storing information collected during border clearance processes were designed to retain that information indefinitely. The assessors explained during interviews with DIBP staff that the risk of attacks to DIBP's databases increases at a rate that is commensurate with the increase in volume of personal information held in these databases.

Privacy issues — destruction and de-identification

8.65 The assessors acknowledge that there may be future uses of the information retained in the DIBP database that necessitate the retention of this information for an extended period of time (refer to Part 7 of this report).

8.66 However, the assessors consider that there is a medium risk of breaching APP 11 resulting from the absence of a destruction policy in relation to information collected during border clearance processes. The assessors note that a destruction policy would need to take into account requirements under the *Archives Act 1983* and any other legal requirements.

8.67 Recommendation 3 addresses this risk.

Part 9: Summary of recommendations

Recommendation 1 — Establish policy governance ownership

9.1 The assessors recommend that DIBP introduces governance measures to ensure an appropriate level of responsibility and accountability for the oversight and implementation of practices, procedures and systems for handling personal information during border clearance processes in accordance with Schedule 5 of the Foreign Fighters Act.

9.2 DIBP accepts this recommendation.

Recommendation 2 — Enhance privacy notification

9.3 The assessors recommend that DIBP enhances its privacy notifications in the departures hall at Brisbane Airport and consider the application of similarly enhanced privacy notifications across all Australian airports.

9.4 DIBP accepts this recommendation, and has already taken steps to address this issue.

Recommendation 3 — Review and/or create documented policies, practices and procedures

9.5 The assessors recommend that DIBP reviews and, where necessary, creates documentation that governs the handling of personal information during border clearance processes in accordance with Schedule 5 of the Foreign Fighters Act. The assessors recommend that the documentation to be reviewed and/or created includes, but is not limited to:

- policies on the destruction or de-identification of information collected during border clearance processes
- training and guidance for DIBP staff and ABF officers on any privacy risks that arise throughout the flow of information collected during border clearance processes and how to mitigate them
- a response plan for incidences of a data breach.

9.6 DIBP accepts this recommendation.

Recommendation 4 — Review ICT security policies, practices and procedures

9.7 The assessors recommend that DIBP reviews its policies, procedures and systems in relation to the ICT security of personal information collected during border clearance processes, particularly in relation to manual information handling processes and data encryption.

9.8 DIBP accepts this recommendation.

Recommendation 5 — Review third party provider access

9.9 The assessors recommend that DIBP reviews its policies, procedures and systems in relation to the levels of access that are granted to third party providers supporting the automated border clearance process.

9.10 DIBP accepts this recommendation.

Recommendation 6 — Enhance physical security at departures SmartGates

9.11 The assessors recommend that DIBP enhances the physical security of the departures SmartGates desk area and the OPC box as necessary to prevent persons being able to view personal information, written or visual.

9.12 DIBP accepts this recommendation, and has already taken steps to address this issue.

Appendix A: Documents provided by DIBP

- Privacy statement
- SmartGate FAQs, viewed 19 February 2016 <http://www.border.gov.au/FAQs/Pages/What-happens-after-I-pass-through-arrivals-SmartGate.aspx>
- Fact sheet — Biometrics, viewed 19 February 2016 http://www.border.gov.au/about/corporate/information/fact-sheets/84biometric>
- DIBP Privacy Policy, viewed 19 February 2016 <http://www.border.gov.au/about/access-accountability/plans-policies-charters/policies/privacy>
- PAM3: Act — Identity, biometrics and immigration status: Collecting personal identifiers onshore
- PAM3: Act — Identity, biometrics and immigration status: Identity information — Access and disclosure
- Australian Border Force Departure SmartGates Business Process Training — Facilitator Guide
- Instrument of Authorisation 2016/001
- Detention Services Manual, Chapter 3 — Entering and leaving detention: Identification tests
- Privacy Impact Assessment — Identifying persons in Immigration Clearance — Schedule 5 — Counter Terrorism Legislation Amendment (Foreign Fighters Act) 2014
- Airport Biometrics Enrolment User Guide (v 4.0)
- Airport Biometric Enrolment diagram
- Passengers Enabling Future Traveller System Biometric Data Retention Policy (SmartGate and Primary Line)
- Outgoing Passenger Card, obtained at Brisbane Airport on 29 February 2016
- Incoming Passenger Card, obtained at Brisbane Airport on 29 February 2016

Appendix B: 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