

The Auditor-General
Audit Report No.33 2011–12
Performance Audit

Management of ePassports

Department of Foreign Affairs and Trade

© Commonwealth
of Australia 2012

ISSN 1036-7632

ISBN 0 642 81240 3

COPYRIGHT INFORMATION

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth.

Requests and inquiries concerning reproduction and rights should be addressed to:

Executive Director
Corporate Management Branch
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email:
webmaster@anao.gov.au

Canberra ACT
22 May 2012

Dear Mr President
Dear Madam Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Department of Foreign Affairs and Trade in accordance with the authority contained in the Auditor-General Act 1997. I present the report of this audit, and the accompanying brochure, to the Parliament. The report is titled *Management of ePassports*.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's Homepage—<http://www.anao.gov.au>.

Yours sincerely



Ian McPhee
Auditor-General

The Honourable the President of the Senate
The Acting Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:

**The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601**

Telephone: (02) 6203 7505

Fax: (02) 6203 7519

Email: webmaster@anao.gov.au

ANAO audit reports and information about the ANAO are available at our internet address:

<http://www.anao.gov.au>

Audit Team

Tim O'Brien

Troy Kelly

William Na

Tom Clarke

Contents

Abbreviations.....	7
Glossary	8
Summary and Recommendations	11
Summary	13
Introduction	13
Audit objective and scope	15
Overall conclusion.....	15
Key findings.....	17
Summary of agency response	22
Recommendations	23
Audit Findings	25
1. Background and Context	27
Introduction	27
International requirements	29
The Australian ePassport.....	30
Facial recognition and the passport issuing process	33
The audit	33
2. Meeting International Requirements	36
Meeting international requirements for ePassports	36
Coordination and information sharing within Australia.....	40
3. Management and Operation of the Facial Recognition System	47
The passport issuing process—overview	47
Management of the facial recognition system	48
Operation of the facial recognition system.....	59
4. The Impact of Facial Recognition Matching on Passport Fraud	65
The nature of passport fraud.....	65
The incidence of passport fraud.....	67
The impact of facial recognition matching on passport fraud	70
5. Securing the ePassport's Microchip and Protecting Privacy	73
Securing and verifying ePassport data	73
Managing privacy aspects of ePassports	81
6. Monitoring ePassport Vulnerabilities and Client Satisfaction.....	87
Vulnerability testing and risk management	87
Monitoring client satisfaction and APO performance	95

Appendices	105
Appendix 1: Agency Response	107
Appendix 2: Passport timeline	109
Appendix 3: Passport issuing process.....	110
Index.....	112
Series Titles.....	113
Current Better Practice Guides	117

Tables

Table 1.1	Passport Redevelopment Program—key elements	29
Table 1.2	Report structure	35
Table 2.1	Examples of APO's international engagement.....	39
Table 2.2	Key interdepartmental meetings and similar activities	41
Table 5.1	Electronic measures to enhance the security of the Australian ePassport.....	74
Table 6.1	Key passport fraud risks and treatments	93
Table 6.2	APO's 2010–11 Key Performance Indicators (KPIs).....	100
Table 6.3	Business Assurance Unit's monthly facial recognition checks.....	102

Figures

Figure 1.1	Number of passports issued each year	27
Figure 1.2	Geographic spread of APO offices in Australia	28
Figure 1.3	Examples of the Australian ePassport's security features	31
Figure 1.4	Number of Australian passports on issue.....	32
Figure 2.1	Case study—Inter-agency cooperation in detecting identity crime	45
Figure 3.1	Passport issuing process.....	47
Figure 3.2	Australian passport photograph guidance	55
Figure 3.3	Percentage of images complying with standards as tested by automated image software	56
Figure 3.4	Facial recognition gallery showing potential matches	60
Figure 4.1	Key emerging passport fraud trends	67
Figure 4.2	New fraud cases (by detection method).....	68
Figure 4.3	Fraud cases <i>recorded</i> as being detected by FR matching.....	71
Figure 5.1	Potential methods of defeating the BAC encryption system	75
Figure 5.2	The public key infrastructure process.....	77
Figure 6.1	Parliamentary Joint Committee Intelligence and Security—Question on Notice (28 August 2008)	91
Figure 6.2	Examples of APO brochures to support client service	96
Figure 6.3	Monthly percentage of passports spoiled and x-spoiled 2010–11	98
Figure 6.4	KPI—10-day target for issuing passports.....	101

Abbreviations

AFP	Australian Federal Police
APO	Australian Passport Office
BAC	Basic Access Control
CSCA	Country Signing Certificate Authority
DFAT	Department of Foreign Affairs and Trade
DIAC	Department of Immigration and Citizenship
DSC	Document Signing Certificate
DSD	Defence Signals Directorate
FR	Facial recognition
ICAO	International Civil Aviation Organization
ISO	International Organization for Standardization
KPI	Key Performance Indicator
NPA	Note Printing Australia
OFPC	Office of the Federal Privacy Commissioner
PICS	Passport Issue and Control System
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification

Glossary

Algorithm	A limited sequence of instructions that tells a computer system how to solve a particular problem, such as generating biometric templates and comparing them.
Biometrics	Automated methods of recognising an applicant based on measurable biological characteristics such as the face or fingerprints.
Eligibility Officer	APO staff responsible for processing passport applications and making decisions about eligibility.
ePassport	A machine readable passport containing a contactless Radio Frequency Identification microchip on which data is stored and protected by Public Key Infrastructure.
Enrolment	The process of collecting a biometric sample from an applicant, converting it into a biometric template and storing it in a database for future comparison.
Facial recognition	A biometric modality that uses an image of a person's face to create a template for recognition purposes.
Gallery	A filtered subset of the APO's facial recognition database that is displayed to Eligibility Officers for assessment against the applicant's image.
Live capture	A process to capture the presenting applicant's image at the time of application.
Note Printing Australia	The organisation contracted by the APO to design and produce passport booklets.
Passport Issue and Control System	An internal APO information technology system that supports passport processing and the storage of personal passport data.
Probe	An image submitted by the applicant used to match against enrolled images in the APO's facial recognition database.

Public Key Infrastructure	A set of policies, processes and technologies used to verify, enrol and certify users of a security application. PKI uses public key cryptography and key certification practices to verify and validate the authenticity and security of a particular system.
Radio Frequency Identification	Radio Frequency Identification involves the use of a wireless non-contact system that uses radio waves to transfer data from a microchip to a microchip reader for the purposes of automated identification.
Template	A mathematical representation based on measurements of an applicant's biometric characteristics.
Threshold	A benchmark score set by the user above which the match between the stored biometric and the applicant is considered to have occurred or below which it is considered not to have occurred. The matching process is determined by the user settings, which can be adjusted so that the biometric system can be more or less strict, depending on the application of the system.
Verification	A task where the biometric system attempts to confirm an applicant's claimed identity by comparing the image with one or more images previously enrolled.
Vulnerability	The potential for a system, such as the APO's facial recognition system or the ePassport's microchip, to be compromised by fraudulent intent, hardware failure or design flaws.
Watchlist	A database of enrolled individuals who are the subject of closer scrutiny prior to approval of a passport issue.

Summary and Recommendations

Summary

Introduction

1. The Department of Foreign Affairs and Trade (DFAT) is responsible for advancing the interests of Australia and Australians overseas. This includes administering the Australian Government's Passport Services Program, which seeks to provide Australians with access to secure international travel documentation through the delivery of high-quality passport services.
2. The Program is expected to cost \$201.7 million in 2011–12 and is administered by the Australian Passport Office (APO), which has some 580 staff located in Canberra and across its network of offices in Australia. Demand for passports has increased in recent years with the number of passports issued each year almost doubling since 2002–03 (from 0.9 million in 2002–03 to 1.8 million in 2010–11). At the same time, the APO has improved the passport booklet's security features and the integrity of the passport issuing process. As part of this ongoing process, in 2010–11, the APO was provided with \$100.8 million over six years for the Passport Redevelopment Program, to deliver a new passport issuing system to enhance the security and efficiency of passport operations.
3. Australian passports currently cost \$233 for an ordinary adult passport¹ and are regarded internationally as high-quality identity documents. The latter is a key reason why Australians are granted visa-free travel to a number of overseas countries. In addition to their primary purpose of facilitating international travel, passports are increasingly used by their holders as personal identification to facilitate everyday transactions. However, if lost, stolen or otherwise fraudulently obtained, passports can be used by fraudsters to establish false identities and facilitate financial crime or other crime such as people smuggling or terrorist acts.
4. Since the September 11 2001 terrorist attacks in the United States of America (USA), there has been an increased focus around the world on strengthening identity security, including the security of international travel documents. A key initiative in improving document security has been the

¹ Different fees apply for seniors, children and frequent travellers, as well as for replacement passports and priority passport processing.

introduction of the ePassport. ePassports contain a microchip which stores a digital photograph and other personal details of the passport holder. The microchip adds additional security features to the booklet which are intended to make the document more difficult to fraudulently produce. In implementing ePassports, countries are required to meet international standards established by the International Civil Aviation Organization (ICAO).

5. Another key driver for Australia's introduction of ePassports was its participation in the USA's Visa Waiver Program. This program allows Australian citizens, in certain circumstances, to enter the USA without first obtaining and paying for a visa. To remain eligible for the program, participating countries were required to introduce ePassports by 26 October 2006.

6. The first Australian ePassport (the 'M' series) was introduced on 24 October 2005. This was replaced by the 'N' series ePassport in May 2009, which further enhanced the document's electronic and physical security features. The next ePassport—the 'P' series—is currently under development with an expected release date between March and May 2014.

7. At the same time as implementing the ePassport in 2005, the APO sought to strengthen its passport issuing process by taking advantage of the passport's biometric capabilities. The APO introduced facial recognition (FR) matching into its eligibility assessment process to reduce the incidence of passport fraud. The FR check seeks to identify potentially fraudulent passport applications by identifying those who might already hold a passport in a different name. While an important function, it is one of about 200 checks performed to verify an applicant's identity and confirm their eligibility for a passport.

8. The digital image on the microchip allows interaction with biometric-based systems that are used by border control officials. The Australian system, known as SmartGate, converts the digital image on the microchip into a biometric template. This template is then compared to a second template created from a live photograph of the passport holder presenting the booklet at the border. This form of biometric matching is

intended to both enhance identity verification and improve the efficiency of passenger processing.²

Audit objective and scope

9. The objective of the audit was to assess the effectiveness of DFAT's implementation of biometric technology to meet international requirements for enhanced passport security. In particular, the audit examined whether:

- Australian ePassports meet international requirements, and coordination with Australian stakeholders is effective;
- Australian biometric passport technology is fit for purpose and has enhanced passport security;
- personal data on the passport microchip is secure and DFAT maintains an appropriate focus on both protecting privacy and client satisfaction; and
- arrangements are in place to evaluate the effectiveness of the ePassport and to monitor risks.

Overall conclusion

10. The implementation and management of biometric technology by passport issuing authorities around the world is a relatively new and challenging function, particularly given the ePassport's dual aims of enhancing passport security and improving the efficiency of passenger processing at the border. In Australia, the task of introducing ePassports occurred against a backdrop of increasing general demand for passports by Australian travellers. Today, there are more than 8.8 million Australian ePassports on issue which represents over 78 per cent of all Australian passports in circulation.

11. The ANAO concluded that the APO has effectively implemented biometric technology and met international requirements and standards for enhanced passport security, while playing an active and influential role in developing these standards. With the introduction of the Australian ePassport on 24 October 2005, Australia became one of the first countries to introduce an ePassport, comfortably meeting the USA's Visa Waiver Program deadline. The

² The ANAO is currently undertaking a performance audit of the Australian Customs and Border Protection Service's processing of incoming international air passengers.

APO's relationships with key Australian stakeholders are collegial and cooperative in nature.

12. The ePassport's electronic security measures, combined with the booklet's security features, make the task of producing a fraudulent passport significantly more complex than it was prior to the ePassport's introduction. There are no known instances of data on the Australian ePassport's microchip being altered, and only one microchip has been found to have failed due to an inherent fault. Overall, the Australian ePassport has helped shift the focus of fraudsters from attempting to alter passport booklets to attempting to fraudulently obtain genuine passports.

13. Although not an international requirement, the APO has incorporated FR matching into its passport issuing process to improve identity verification and reduce the incidence of passport fraud. In this regard, the FR system has detected many cases of identity fraud that would not otherwise have been detected.

14. While the introduction of Australian ePassports has been generally sound, there are a number of weaknesses in some of the APO's supporting administrative arrangements that have the potential to impede effective management decision-making and the monitoring and reporting of outcomes. In particular, while a timely review of the FR system was undertaken in 2008, most of the review observations and recommendations had still not been addressed in 2011. Weaknesses remained in the general system documentation, documentation relating to the testing and approval of FR system settings, and the training and guidance material available to staff involved in FR matching. During the audit the APO developed a plan to take these outstanding issues forward, but this is an area that would benefit from active management oversight.

15. At the time of the audit there were difficulties in extracting accurate data from the APO's systems on passport fraud, which weakens the assurance that the nature and incidence of that fraud has been carefully monitored and accurately reported. In particular, the incorrect recording of the detection method for some FR matches impairs the APO's ability to accurately quantify the success of the FR system in detecting fraud. The APO has work underway to address these weaknesses.

16. Furthermore, while the Defence Signals Directorate (DSD) has advised the ANAO that the microchip's electronic security features should be moderately secure provided they have been applied effectively, at the time of

the audit the APO had not conducted independent vulnerability testing of the application of these security features. While DSD has now been engaged to carry out this testing, there would be merit in the APO periodically reviewing the need for further vulnerability testing in consultation with DSD. With regard to the monitoring of more general passport risks, the APO did not have an up-to-date formal risk management plan covering its key strategic and operational risks at the time of the audit. However, it has now developed a strategy to manage these risks.

17. The APO consistently meets its target of issuing passports within 10 working days and was able to maintain its performance against this target during the introduction of the ePassport. However, there are opportunities to develop a broader range of quantitative and qualitative indicators for assessing passport integrity and performance. The APO has agreed to establish new indicators to monitor performance.

18. Overall, the APO has been responsive to the issues raised during the audit. In view of the work commenced or outlined by the APO to address these issues, the ANAO has made only two recommendations aimed at further strengthening the APO's management of ePassports.

Key findings

Meeting International Requirements

19. The introduction of the Australian ePassport in 2005 was driven by two key international requirements: the need to comply with various international standards for ePassport design; and the desire to continue Australia's participation in the USA's Visa Waiver Program, which facilitates the travel of Australian citizens to the USA.

20. The APO assisted in developing international standards for ePassports—including the use of the face as the primary biometric, microchip standards and electronic measures to secure the microchip data—and has successfully implemented the key features required in the Australian ePassport.

21. The management of border and identity security is a collaborative effort between federal and state government agencies. To this end, the APO actively participates in relevant interdepartmental activities, promotes its FR capabilities as a resource to assist national law enforcement, and has entered into a mutually beneficial arrangement with the Australian Federal Police for the secondment of a police officer to its Sydney office. Overall, these

arrangements indicate a mature and appropriate coordination approach with stakeholders.

22. Notwithstanding this approach, there are opportunities for the APO to strengthen its interaction with stakeholders. In particular, the development of a joint strategy with the Australian Customs and Border Protection Service (Customs and Border Protection) would enable the incidence of ePassports that fail to read at the border to be better measured and managed. In response to this suggestion, the APO and Customs and Border Protection agreed that a joint strategy would be beneficial, with the APO advising that it will seek to establish a joint working group to manage relevant border issues. At the time of the audit, the APO's strategic intelligence capability was limited, but the APO had already flagged an intention to reinvigorate this capability.

Management and Operation of the Facial Recognition System

23. The APO is continually improving and strengthening its passport issuing process in an effort to ensure that Australian passports are only issued to persons who are entitled to hold them. At the time of the audit, it conducted about 200 checks in assessing an applicant's eligibility and in validating supporting information. With the introduction of ePassports and FR technology in October 2005, the APO introduced an additional eligibility check to reduce the incidence of passport fraud. This involves matching the applicant's image against other images held in its passport database to reduce the risk that the applicant has already been issued with a travel document in another name.

24. FR matching is not an international requirement and Australia was one of the first countries to introduce it into its passport issuing process. However, most observations and recommendations from a 2008 review of the APO's FR system, including key system documentation and reducing the APO's reliance on an individual officer for system maintenance and support, had still not been addressed in 2011. The APO has since engaged a contractor to document its FR systems, and developed a strategy to overcome this potential single point of failure. It has also developed a Future Directions Plan to take other outstanding issues forward. However, this is an area that would benefit from ongoing active management oversight and periodic progress review, to ensure that key issues are addressed in a timely manner.

25. The APO uses a commercially supplied biometric algorithm to convert passport photographs into templates and to compare the applicant's template to all other templates in its database. The FR system has been updated for new

algorithms, but the APO was unable to locate documentation of its testing methodology in comparing the effectiveness of the new and old algorithms, and the consideration of change proposals by management. In response, the APO advised that the methodology is now being documented and a health check of the FR system will be undertaken in the first half of 2012.

26. As part of this process, it will also be important for the APO to develop and document a mechanism for ongoing assessment and adjustment of the FR system settings and monitoring of outcomes, to help optimise system performance. This approach will better equip the APO Senior Executive to weigh future trade-offs between staff workload and the probability of fraud detection. Documenting management's consideration of proposed changes to system settings will also strengthen accountability and facilitate future review.

27. The APO uses people to visually inspect and verify submitted photographs against international standards, and considers that it meets all international requirements in this regard. While automated image checking software has the potential to improve image quality and the effectiveness of FR technology during application processing and at the border, it is not an international requirement nor is it practical to implement at this time. Its use would only be possible if the APO changed from its current process of scanning submitted photographs to the live capture of digital images. The APO intends to pilot live capture as part of its Passport Redevelopment Program.

28. The FR system identifies potential matches and presents those in a gallery for an APO Eligibility Officer to consider whether any require more detailed investigation by the fraud unit. While the FR gallery user interface has been improved since its introduction in 2005, it remains difficult for Eligibility Officers to use efficiently and effectively. The APO expects to redesign, test and deploy an enhanced FR gallery in the first half of 2012, to overcome these issues.

29. Appropriate and up-to-date training and guidance material is important to support staff involved in the FR matching process. While weaknesses in both areas were apparent at the time of the audit, the APO was taking steps to overcome them. In particular, it advised that it will update its FR training and guidance material, and develop a medium to long-term training strategy by June 2012. In addition, the APO will consider introducing periodic mandatory training and assessments for staff involved in FR decision-making, and advised that it has now put in place a system to automatically record the completion of training modules. The APO is also

funding research work that should provide useful information on how to optimise Eligibility Officers' training and help improve their performance in matching faces.

The Impact of Facial Recognition Matching on Passport Fraud

30. The number of new passport fraud cases detected by the APO and other agencies increased from 178 in 2003–04 to 849 in 2010–11. The APO attributes this increase to the growing number of passports issued and to its greater investigative capability rather than to an increase in the rate or incidence of fraud per se.

31. FR matching has been attributed as detecting on average about 22 cases of fraud a year since its introduction. However, this figure is understated by an unknown amount because of the incorrect recording of the detection method for some FR matches.

32. The APO advised that a new case management system ('eCase') being developed as part of the Passport Redevelopment Program, and an interim solution that was implemented in February 2012, will enable the accurate recording and extraction of fraud statistics in the future.

Securing the ePassport's Microchip and Protecting Privacy

33. The ePassport employs a number of electronic security features to protect the personal information stored on the microchip against a range of potential threats. While media reports have suggested that the personal information on the microchip is vulnerable to unauthorised access and copying, there are no known instances of fraudsters successfully overcoming the electronic security features of the Australian ePassport.

34. With around 48 per cent of the Australian population holding a passport, the APO holds significant amounts of personal information in its passport systems, including biometric information. It is therefore important that appropriate measures are employed to secure this information and protect holders' privacy in accordance with the *Privacy Act 1988*. To this end, the APO put in place effective arrangements to manage the privacy of individual passport holders following the introduction of ePassports in 2005, and the Office of the Australian Information Commissioner has not received a complaint about the APO since that time.

35. The APO's key system for storing personal details is the Passport Issue and Control System (PICS). While access to PICS is logged in an electronic

audit trail, the APO does not proactively use this facility to identify potentially inappropriate database access. A small number of periodic random audits would increase management's assurance that access to personal records is appropriate. The APO does monitor staff access to the records of a limited number of passport holders whose records are considered to be at higher risk of inappropriate access. However, the arrangement and the criteria used for adding or removing passport holders to this list have not been documented.

36. The APO Canberra conducts a structured induction program that includes a mandatory requirement for new staff to complete a self-paced online privacy module. However, at the time of the audit, privacy refresher training was not mandatory, nor was a record kept of those who had undertaken it. The APO advised that it has now developed a system to identify staff requiring refresher training and to record its completion.

Monitoring ePassport Vulnerabilities and Client Satisfaction

37. The insertion of microchips into passport booklets introduced the potential for microchip failure and inconvenience to the passport holder. Therefore, it is important that the microchip is sufficiently robust to survive the rigours of passport production and use, for its 10-year life. The APO has adopted a sound approach to managing the risk of microchip failure, including testing its robustness during the development of the first 'M' series ePassport and obtaining a 12-year warranty from the microchip manufacturer. Only one microchip has been found to have failed due to an inherent fault (out of more than 8.8 million ePassports that have been issued).

38. The APO has also adopted a sound approach to testing the physical security features of the passport booklet, but relies on internationally proven electronic security features to protect the embedded microchip. At the time of the audit the APO had not conducted independent vulnerability testing of their application but, in response to these findings, has now engaged DSD to carry out this testing. The need for further vulnerability testing should be periodically reviewed in consultation with DSD to identify emerging threats, with future independent vulnerability testing to be conducted as required.

39. The APO has included key passport fraud risks in the DFAT-wide Fraud Control Plan, and seven strategic risks in the DFAT-wide Risk Register. However, at the time of the audit, the APO did not have an up-to-date formal risk management plan covering its key strategic and operational risks, which would assist with their regular and systematic review. In response, the APO

advised that it has now developed a risk strategy to actively manage its strategic and operational risks.

40. The APO has established a Client Service Charter that outlines service standards and has developed a series of supplementary brochures that provide information to clients on their rights and responsibilities. While client feedback is collected through a number of specific initiatives, at the time of the audit there was no centralised collection or analysis of feedback that is provided by clients at the APO's network of offices. However, during the audit the APO developed a new feedback policy to identify and share better practice and lessons learned across the APO network.

41. The APO consistently meets its target of issuing passports within 10 working days (average of 3.7 days in 2010–11) and was able to maintain its performance against this target during the introduction of the ePassport in 2005–06 (average of 4.1 days in that year). However, there are opportunities to develop a broader range of quantitative and qualitative indicators for assessing passport integrity and performance and for reporting on the performance of the FR system to the Senior Executive. The APO has agreed to establish new indicators to monitor performance.

Summary of agency response

42. The proposed report was provided to DFAT for comment. DFAT's full response to the audit is at Appendix 1. Its summary response is as follows:

DFAT welcomes the findings of the ANAO report into the management of ePassports. Australia was instrumental in the development of the international standards for the ePassport and in 2005 was one of the first countries to introduce a compliant ePassport. The report acknowledges that DFAT has effectively implemented biometric technology and met the international requirements and standards for enhanced passport security. The report confirms that the ePassport's electronic security measures, combined with the booklet's security features, make the task of producing a fraudulent passport significantly more complex.

DFAT was a pioneer in the use of facial recognition matching in the passport assessment process and remains a world leader in its use. The report acknowledges that, while not an international requirement, DFAT has incorporated the facial recognition capability to improve identity verification and reduce the incidence of passport fraud. DFAT agrees with the recommendation to involve the Defence Signals Directorate in vulnerability testing of the ePassport and believes that their involvement will strengthen the integrity of the ePassport program.

Recommendations

Set out below are the ANAO's recommendations aimed at further strengthening the APO's management of ePassports.

Recommendation No.1 To strengthen the management of its facial recognition system, the ANAO recommends that the APO:

Para 3.39

Facial Recognition

- periodically review progress in addressing the outstanding observations and recommendations identified in 2008 so that key issues are dealt with in a timely manner; and
- develop and document a mechanism for the ongoing assessment and adjustment of the facial recognition system settings and document management's consideration of future proposed changes to those settings.

DFAT response: *Agreed.*

Recommendation No.2 To strengthen the management of the ePassport's electronic security features, the ANAO recommends that

Para 6.30

Vulnerability Testing

the APO periodically review, in consultation with the Defence Signals Directorate, the need for further vulnerability testing of the application of these measures and, if required, arrange appropriate independent testing.

DFAT response: *Agreed.*

Audit Findings

1. Background and Context

This chapter provides an overview of the introduction of ePassports by the Department of Foreign Affairs and Trade. It also outlines the audit approach.

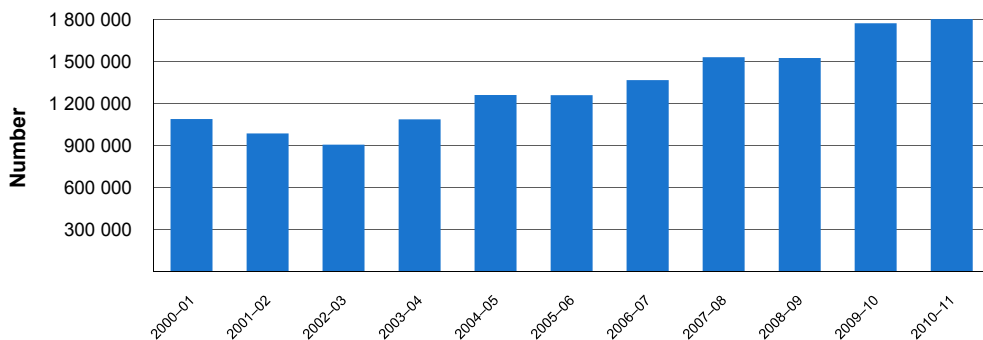
Introduction

1.1 The Department of Foreign Affairs and Trade (DFAT) is responsible for advancing the interests of Australia and Australians overseas. This includes administering the Australian Government's Passport Services Program, which seeks to provide Australians with access to secure international travel documentation through the delivery of high-quality passport services. Passport services are expected to cost some \$201.7 million in 2011–12.

1.2 The demand for Australian passports has increased since 2002, driven in part by the strength of the Australian economy. The number of passports issued each year has almost doubled since 2002–03 (see Figure 1.1), with the number on issue increasing from 7.6 million to 11.0 million over the same period. By 2010–11 around 48 per cent of Australian citizens held a passport (up from 37 per cent in 2002–03). Applicants pay a fee of \$233 for an ordinary adult passport³ which has a life of 10 years.

Figure 1.1

Number of passports issued each year



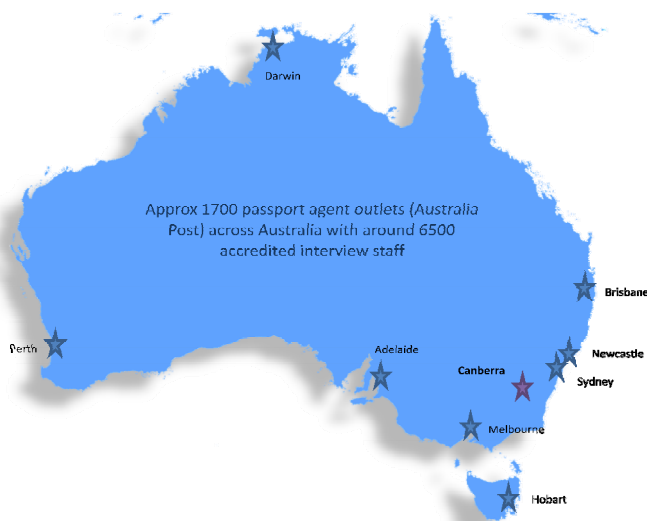
Source: DFAT Annual Reports.

³ Different fees apply for seniors, children and frequent travellers, as well as for replacement passports and priority passport processing.

1.3 In July 2006, DFAT created the Australian Passport Office (APO) as a separate division to administer the Passport Services Program. At the time of the audit, the APO had some 580 staff located across Australia. The APO's headquarters are in Canberra and it has offices in each of the state and territory capital cities and one in Newcastle (see Figure 1.2). Certain passport services are also provided at Australian diplomatic missions overseas.

Figure 1.2

Geographic spread of APO offices in Australia



Source: Australian Passport Office.

1.4 Australian passports are regarded internationally as high-quality identity documents. This is a key reason why Australians are granted visa-free travel to a number of overseas countries. In addition to their primary purpose of facilitating international travel, passports provide personal identification for people seeking access to a range of government and non-government services and benefits and are used to facilitate everyday transactions. However, if lost, stolen or otherwise fraudulently obtained, passports can be used by fraudsters to establish false identities and facilitate financial crime or other crime such as people smuggling or terrorist acts.

1.5 The security of the passport booklet and the passport issuing process are important to provide confidence that passport holders are who they claim to be, and have a legitimate right to enter and leave Australia. The challenge for the APO is to balance the efficient issuing of passports to meet the increasing demand, while implementing effective strategies to maintain the integrity of the document itself.

1.6 To this end, the APO has an ongoing program to improve the booklet's security features (through the issuing of new booklet series) and the integrity of the passport issuing process. As part of this ongoing process, in the 2010–11 Budget, the APO was provided with \$100.8 million over six years for the Passport Redevelopment Program, which will deliver a new passport issuing system to enhance the security and efficiency of passport operations. Key elements of the Program are outlined in Table 1.1.

Table 1.1

Passport Redevelopment Program—key elements

Element	Planned outcomes
eCapture	To capture all data and images required to support an application for an Australian travel document.
eFlow	To manage the collection, movement and assessment of data required to authorise the issue of an Australian travel document. eFlow is the central component in the overall solution and will operate in concert with other elements to provide the overarching workflow.
eCase	To provide an enhanced investigation, analytical, intelligence and case management capability to contribute to the security and issuing of Australian travel documents.
ePrint	To manage the personalisation and printing of Australian travel documents, including microchip encoding, automated inspection and quality assurance and production of standard letters to applicants.

Source: ANAO representation of the Passport Redevelopment Program Business Case.

International requirements

1.7 Since the September 11 2001 terrorist attacks in the United States of America (USA), there has been an increased focus around the world on strengthening identity security, including the security of international travel documents. The Australian Government's National Identity Security Strategy sees identity security as central to Australia's national security, law enforcement and economic interests. The security features and enrolment procedures around identity credentials, such as the Australian ePassport, are key elements of the strategy.⁴

1.8 A key initiative in improving international travel document security has been the introduction of the ePassport. Australian ePassports contain a

⁴ The development of this strategy was examined in ANAO Audit Report No.29 2009–10, *Attorney-General's Department Arrangements for the National Identity Security Strategy*.

Radio Frequency Identification (RFID) microchip in the centre page of the passport booklet.⁵ The microchip stores a digital photograph of the holder, as well as the holder's name, sex, date of birth, nationality, passport number and passport expiry date.⁶ The inclusion of the microchip adds additional security features to the booklet, and is intended to make the document more difficult to produce fraudulently.

1.9 Another key driver for Australia to introduce ePassports was its participation in the USA's Visa Waiver Program. This program allows Australian citizens, in certain circumstances, to enter the USA without first obtaining and paying for a visa. Following September 11, the USA passed legislation that required countries eligible for the Visa Waiver Program to introduce ePassports by 26 October 2006 to remain eligible.⁷

1.10 In implementing ePassports, countries are required to meet international standards for global travel documents that are established by the International Civil Aviation Organization (ICAO).⁸

The Australian ePassport

1.11 The first Australian ePassport (the 'M' series) was introduced on 24 October 2005. This was replaced by the 'N' series ePassport in May 2009, which further enhanced the document's electronic and physical security features. Figure 1.3 illustrates some of the passport booklet's security features, which include the use of specialised materials, and complex printing and document construction processes. The next ePassport—the 'P' series—is currently under development with an expected release date between March and May 2014. An outline of key events in recent years is at Appendix 2.

⁵ RFID devices transmit data to reading devices using an electromagnetic field. The ePassport's RFID microchip is a passive device, which means that it generates its energy from the electromagnetic field of the reader.

⁶ Most of this data is also contained on the printed biographical data page of the passport booklet.

⁷ The original United States Visa Waiver Program deadline for the implementation of the ePassport was 26 October 2004. However, this was postponed twice until the final deadline of 26 October 2006.

⁸ As at 29 July 2011, 93 nations were issuing ePassports and a further 21 had plans to issue ePassports before the end of 2011.

Figure 1.3**Examples of the Australian ePassport's security features**

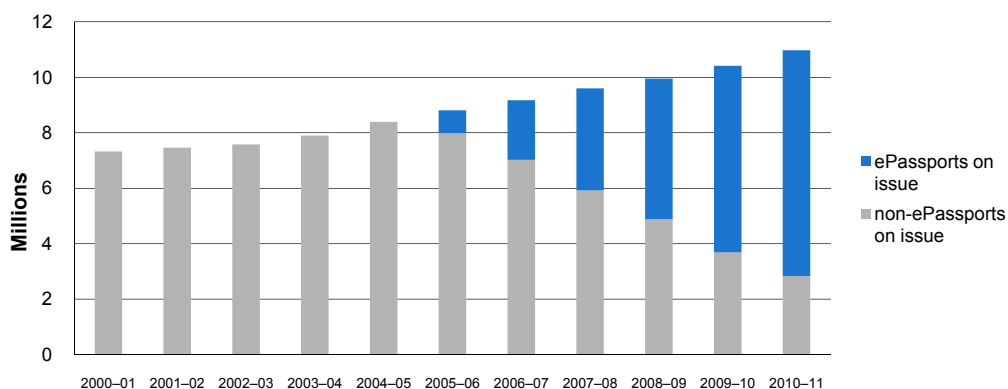
Source: ANAO representation.

1.12 Unless otherwise cancelled or invalidated passports issued by the APO remain valid until their expiry date. As the Australian passport is generally valid for a 10-year period, non-ePassports issued prior to October 2005 may continue to be used by those holding them. While each passport series seeks to enhance security, all valid passports remain protected by the physical security features relevant to its passport series. As shown in Figure 1.4, the number of valid non-ePassports on issue will continue to fall until the last expires in October 2015. As at 31 January 2012, there were more than 8.8 million

ePassports on issue, which constituted over 78 per cent of the 11.3 million in circulation.

Figure 1.4

Number of Australian passports on issue



Source: ANAO analysis of APO data.

1.13 The ePassport is often inaccurately described as a biometric passport. While ICAO standards require a digital image to be stored on the microchip, there is no biometric data (measurement of a physical feature)⁹ contained on the microchip. However, the digital image on the microchip allows interaction with biometric-based systems that are used by border control officials. At the border, the biometric system converts the digital image on the microchip into a biometric template. This template may then be compared to a second template created from a live image of the passport holder presenting at the border. This form of biometric matching is intended to enhance identity verification processes and is considered to be more efficient than traditional visual matches made by border officials. It also improves the efficiency of passenger processing.

1.14 In Australia, responsibility for border control rests with the Australian Customs and Border Protection Service (Customs and Border Protection). Customs and Border Protection has implemented an automated border control system known as SmartGate, which includes the use of biometric technology to

⁹ Biometrics refers to identification of individuals based on intrinsic physiological characteristics. Common biometric identifiers used are fingerprints, DNA, and facial and iris recognition.

verify the identity of travellers. Certain Australian and New Zealand ePassport holders may elect to use SmartGate¹⁰ or to be manually processed by a Customs and Border Protection official. Where SmartGate is unable to verify a person's identity,¹¹ the passport holder is referred for manual processing. Non-Australian and New Zealand ePassport holders must be manually processed.¹²

Facial recognition and the passport issuing process

1.15 At the same time as implementing the ePassport in 2005, the APO sought to strengthen its passport issuing process by introducing facial recognition (FR) matching into its eligibility assessment process to reduce the incidence of passport fraud. The use of FR during the passport issuing process is not an international requirement.

1.16 The APO's FR check seeks to identify fraudulent passport applications by identifying those who might already hold a passport in a different name. Potential matches identified by the FR system are presented to an Eligibility Officer for consideration. It is up to the Eligibility Officer to consider whether any require more detailed investigation by the APO's fraud unit. While the FR check is an important function, it is one of about 200 checks performed to verify an applicant's identity and confirm their eligibility for a passport.

The audit

Audit objective and scope

1.17 The objective of the audit was to assess the effectiveness of DFAT's implementation of biometric technology to meet international requirements for enhanced passport security. In particular, the audit examined whether:

- Australian ePassports meet international requirements, and coordination with Australian stakeholders is effective;
- Australian biometric passport technology is fit for purpose and has enhanced passport security;

¹⁰ SmartGate can generally be used by Australian and New Zealand ePassport holders aged 16 and over.

¹¹ For example, an error may occur due to the passport holder failing to use SmartGate correctly.

¹² The ANAO is currently undertaking a performance audit of the Australian Customs and Border Protection Service's processing of incoming international air passengers.

- personal data on the passport microchip is secure and DFAT maintains an appropriate focus on both protecting privacy and client satisfaction; and
- arrangements are in place to evaluate the effectiveness of the ePassport and to monitor risks.

1.18 The audit focused on the novel aspects of the ePassport's security features and the implementation of FR technology for eligibility checking. In view of the sensitivities surrounding the FR system and the potential for passport fraud, some operational details relating to passport processing arrangements and the operation of the APO's FR technology have been omitted from this report.

1.19 This audit was conducted in parallel with an ANAO performance audit of the Australian Customs and Border Protection Service's processing of incoming international air passengers. Among other things, that audit is reviewing the operation and performance of SmartGate in using the ePassport's technology at the border.

Previous ANAO audits

1.20 The ANAO audited passport services in 2002–03 with the objective of assessing whether DFAT had effective processes for issuing passports in Australia.¹³ In particular, that audit focused on whether DFAT had effective strategies for assessing passport eligibility, securing the passport booklet and monitoring performance and the quality of client service. In addition, in 2007–08 the ANAO undertook an audit of the Department of Immigration and Citizenship's design and planning for the introduction of biometric technologies in that agency.¹⁴

Audit methodology

1.21 In undertaking the audit, the ANAO examined and reviewed DFAT's files and electronic documents, academic papers and reports of other government agencies and international bodies. In addition, the ANAO conducted interviews and observed APO staff processing passport

¹³ ANAO Audit Report No.37 2002–03, *Passport Services*.

¹⁴ ANAO Audit Report No.24 2007–08, *DIAC's Management of the Introduction of Biometric Technologies*.

applications, including reviewing potential FR matches, at its headquarters in Canberra and at its state offices in Melbourne and Sydney.

1.22 The ANAO also consulted with key stakeholders at Customs and Border Protection, the Australian Federal Police, the Department of Immigration and Citizenship, the Department of Defence, the Office of the Australian Information Commissioner and Note Printing Australia.

1.23 The audit was conducted in accordance with the ANAO's auditing standards at a cost of \$350 000.

Report structure

1.24 The audit findings are reported in the following five chapters, which are outlined in Table 1.2.

Table 1.2

Report structure

Chapter 2 Meeting International Requirements	This chapter examines the APO's approach to: <ul style="list-style-type: none"> • Meeting international requirements for ePassports • Coordination and information sharing within Australia
Chapter 3 Management and Operation of the Facial Recognition System	This chapter reviews the: <ul style="list-style-type: none"> • Passport issuing process • Management of the facial recognition system • Operation of the facial recognition system
Chapter 4 The Impact of Facial Recognition Matching on Passport Fraud	This chapter examines: <ul style="list-style-type: none"> • The nature of passport fraud • The incidence of passport fraud • The impact of facial recognition matching on passport fraud
Chapter 5 Securing the ePassport's Microchip and Protecting Privacy	This chapter examines arrangements for: <ul style="list-style-type: none"> • Securing and verifying ePassport data • Managing privacy aspects
Chapter 6 Monitoring ePassport Vulnerabilities and Client Satisfaction	This chapter assesses: <ul style="list-style-type: none"> • Vulnerability testing and risk management • Monitoring client satisfaction and APO performance

2. Meeting International Requirements

This chapter examines the approach taken to meet the requirements for Australian ePassports to comply with international standards for ePassport design and the USA's Visa Waiver Program requirements. It also assesses the APO's approach to managing its key relationships and sharing information within Australia.

Meeting international requirements for ePassports

2.1 The introduction of the Australian ePassport in 2005 was intended to not only enhance passport security and assist automated passenger processing systems, but was also driven by two international requirements. The requirements were the need to:

- comply with various international standards for ePassport design; and
- continue Australia's participation in the Visa Waiver Program to facilitate the travel of Australian citizens to the USA.

2.2 Australia's approach to meeting these requirements is examined in the following section. This section also reviews the arrangements for testing the interoperability of Australian ePassports internationally, and the role that the APO has played internationally in the development and implementation of ePassports.

International standards for ePassport design

2.3 The International Civil Aviation Organization (ICAO) is the international body with responsibility for setting global travel document standards.¹⁵ In order to facilitate the international travel of its citizens, Australia seeks to comply with ICAO standards in the design and features of the Australian ePassport. In 2003 ICAO sought to standardise ePassports

¹⁵ In addition, there are also numerous standards relevant to ePassports set by the International Organization for Standardization (ISO), including printing inks, formats for exchanging biometric data and the design of the microchip and microchip data. The International Electrotechnical Commission (IEC) also plays a part in setting international biometric standards.

issued by its member states by specifying the inclusion of four key features¹⁶:

- the use of the face as the primary biometric identifier (secondary biometrics such as fingerprints or iris are optional);
- the storage of electronic data on a contactless Radio Frequency Identification (RFID) microchip;
- the employment of a standardised logical data structure on the microchip; and
- the use of Public Key Infrastructure (PKI) to detect unauthorised alteration of data (with optional use of Basic Assess Control (BAC) to prevent unauthorised access to the data).

2.4 These requirements were met when Australia launched its 'M' series ePassport on 24 October 2005, becoming one of the first countries to introduce an ePassport. Australia's ePassport uses a facial image as the biometric identifier with the digital image and other biographical data stored on a RFID microchip employing a logical data structure. Australia has implemented BAC to protect the privacy of the passport holder and uses the ICAO specified PKI to provide assurance that the data was written by the authorised agency and remains unaltered.

2.5 The APO advised that there have been no reports from ICAO member states of technical failures relating to Australian ePassports.

USA's Visa Waiver Program requirements

2.6 The USA's Visa Waiver Program allows Australian citizens and those of other participating countries, in certain circumstances, to enter the USA for up to 90 days without first obtaining (and paying for) a visa.¹⁷

¹⁶ See ICAO specifications for Machine Readable Travel Documents, including document 9303 at <<http://www2.icao.int/en/MRTD/Pages/default.aspx>> [accessed 29 November 2011].

¹⁷ The program was introduced in 1986 to eliminate unnecessary barriers to travel, to stimulate the USA's tourism industry, and to permit the USA's Department of State to focus consular resources in other areas (details are at <http://travel.state.gov/visa/temp/without/without_1990.html#vwp> [accessed 29 November 2011]). At the time of this audit, 36 countries were participating in the program. Loss of access to the program would inconvenience hundreds of thousands of Australians who travel to the USA each year.

2.7 One of the initiatives taken by the USA Government to strengthen border security after the terrorist attacks of September 11 2001 was to enact the *Enhanced Border Security and Visa Entry Reform Act* (May 2002). This legislation required countries participating in the program to issue their citizens, by 26 October 2004, with machine readable passports that were tamper-resistant and incorporated a biometric identifier compliant with ICAO standards.

2.8 The deadline for introducing ePassports was twice extended by the USA due to technical issues before coming into effect on 26 October 2006.¹⁸ Valid non-ePassports issued prior to that time may still be used for travel under the program under certain circumstances.¹⁹

2.9 Australia comfortably met the USA's Visa Waiver Program deadline by more than 12 months. By way of comparison, the United Kingdom introduced its ePassport in March 2006 and the USA itself in August 2006. All valid Australian passports currently on issue that precede the ePassport have machine readable zones and therefore also comply with the USA's Visa Waiver Program requirements.²⁰

Interoperability testing

2.10 To allow passport holders to travel unhindered internationally it is important that ePassports are tested to ensure that they can be read by border control agencies around the world.

2.11 To this end, a series of international interoperability trials, endorsed by ICAO and the International Organization for Standardization (ISO), were conducted at various international locations between 2004 and 2008²¹ to enable countries to swap sample ePassports and test the compatibility of their ePassports with readers from a range of manufacturers. The ANAO reviewed APO files and reports relating to these interoperability trials and noted that

¹⁸ The USA extended the deadline for ePassports in July 2004 to 26 October 2005 and in June 2005 to 26 October 2006.

¹⁹ Machine readable passports issued on or after 26 October 2006 must have an integrated microchip with information from the biographical data page. Machine readable passports issued between 26 October 2005 and 25 October 2006 must have a digital photograph printed on the biographical data page or an integrated microchip with information from the biographical data page. Passports issued before 26 October 2005 require nothing other than a machine readable zone.

²⁰ Australia introduced a machine readable zone on its passports in 1986.

²¹ Key interoperability trials were held in Canberra (2004), Morgantown (2004), Sydney (2004), Baltimore (2004), Tsukuba (2005), Singapore (2005), Berlin (2006), and Prague (2008).

Australia actively participated in them and successfully verified the compatibility of Australian ePassports.

2.12 To facilitate the certification of ePassports for the purposes of the USA’s Visa Waiver Program, Australia also participated in international live testing of ePassports being undertaken by the USA’s Department of Homeland Security at two American airports and one Australian airport in 2005 and 2006.²² In December 2005, DFAT received certification from the Department of Homeland Security that Australian ePassports were compatible with the USA’s passport reader technology.

International cooperation and engagement

2.13 The international requirements for ePassport design and compatibility underline the importance of APO being actively engaged with the international community on ePassport issues.

2.14 The ANAO reviewed APO files, international reports, correspondence and ICAO committee papers and documents. The documents show that the APO has played an active and influential role in the development of international standards for ePassports, including the use of the face as the primary biometric, microchip standards and technology and the use of PKI to help secure the electronic data. Examples of the APO’s international involvement, including its participation in ICAO committees and working groups, are outlined in Table 2.1.

Table 2.1

Examples of APO’s international engagement

Example	ANAO comment
Development of ICAO standards for ePassports	<p>The APO actively participated in the development of the 2003 ICAO standards for ePassports.</p> <p>The APO continues to be active in the ICAO New Technology Working Group and the Technical Advisory Group on Machine Readable Travel Documents, which assess and design standards for ePassport interoperability.</p>

²² In addition to the USA and Australia, two of the 27 countries that participated in the USA’s Visa Waiver Program at that time also participated in the trials.

Example	ANAO comment
International Organization for Standardization	The APO represents Australia on several key ISO/IED working groups and related committees including Sub Committee 17 (<i>Cards and Personal Identification</i>) and Sub Committee 37 (<i>Biometrics</i>), which are responsible for setting standards in their respective areas.
Public Key Infrastructure (PKI)	The APO is an active participating member of the Public Key Directory (PKD) and took a lead role in the development and promotion of the PKI in 2007. A senior APO officer was the inaugural chair of the ICAO PKD Board and Australia was one of the six initial participating nations. ²³
Five Nations Passport Conferences (USA, UK, Australia, Canada and NZ)	Australia participates in the Five Nations Biometric Working Group, which shares experiences in implementing FR systems, and the Anti Fraud Working Group, which discusses trends and responses to passport fraud risks.

Source: ANAO analysis of APO documents and publicly available documents.

Conclusion—Meeting international requirements for ePassports

2.15 The APO has been actively involved in the development of international standards for ePassports and has successfully implemented the four key ICAO features in Australian ePassports. Australia was one of the first countries to introduce an ePassport, comfortably meeting the USA's Visa Waiver Program deadline with the introduction of the 'M' series ePassport on 24 October 2005, and thereby facilitating the ongoing travel of Australian citizens to the USA.

Coordination and information sharing within Australia

2.16 As the management of border and identity security is a collaborative effort between federal and state government agencies, it is important that the APO manages its relationships effectively to maintain trust in the security of its identity verification, passport issuing process and the passport document itself.

2.17 To assess the APO's approach to managing its key relationships, the ANAO reviewed its:

- participation in interdepartmental committees and similar activities;
- management of key relationships; and

²³ As at July 2011, 27 countries were active members of the ICAO PKD.

- arrangements for exchanging information with stakeholders.

Participation in interdepartmental committee meetings and similar activities

2.18 Participation in interdepartmental committees facilitates the development of effective strategies to manage whole-of-government issues such as identity crime. The ANAO's review of APO files, meeting minutes, correspondence between stakeholders and meeting with APO staff and key stakeholders indicated the APO to be active in interdepartmental meetings, putting forward suggestions to improve whole-of-government processes and inter-agency cooperation. Some of the key meetings are outlined in Table 2.2.

Table 2.2

Key interdepartmental meetings and similar activities

Activity	ANAO Comment
National Identity Security Strategy	This committee provides a framework for intergovernmental cooperation to combat identity theft and the fraudulent use of stolen and assumed identities. ²⁴
Commonwealth Reference Group on Identity Security	This committee coordinates Australian Government strategies for identity security related matters. It includes a biometrics working group. ²⁵
Document Verification Service	The Service provides participating agencies with access to information to verify the bona fides of identity documents issued by other participating agencies.
Border Management Group	The Border Management Group implements the Government's Strategic Border Management Plan. The Strategic Border Management Plan provides guiding principles for the development of border management initiatives and priorities for addressing risks.
Biometrics Institute activities	The Biometrics Institute is a not-for-profit organisation that promotes the responsible use of biometrics. The Biometrics Institute runs a number of events annually, including training courses, conferences and technology showcases.

Source: ANAO analysis of APO documents.

²⁴ For further information, see ANAO Audit Report No.29 2009–10, *Attorney-General's Department Arrangements for the National Identity Security Strategy*, p.36.

²⁵ *Ibid.*, p.15.

Managing key relationships

2.19 In addition to interdepartmental cooperation, agencies often need to manage bilateral relationships with other agencies to effectively manage specific issues.

2.20 The ANAO's file reviews indicated that the APO actively participated with Customs and Border Protection and the Department of Immigration and Citizenship (DIAC) in planning and implementing the Government's Biometrics for Border Control project.²⁶ In addition, the ANAO met with staff from two APO state offices, Customs and Border Protection, DIAC and the Australian Federal Police (AFP) during the course of the audit. These meetings indicated that there is regular interaction with the APO at the working level and that these relationships are collegial and cooperative in nature.

AFP assistance for passport fraud investigations

2.21 In the past, the AFP was responsible for conducting passport fraud investigations. However, the current model involves the APO carrying much of this workload, which requires effective cooperation to manage, prioritise and coordinate passport fraud cases. Given its role, it is important that the APO actively seeks to develop its skills to conduct specialised investigations.

2.22 In 2010, the AFP conducted a quality assurance review of a fraud investigation by the APO to provide assurance and feedback on the APO's investigative practices. While the review identified some areas for improvement, such as the need to enhance procedural documentation, it concluded that the APO had competent investigators, sound investigative practices and a commitment to improving its systems.

2.23 The APO has also entered into a Memorandum of Understanding (MOU) with the AFP²⁷ for a police officer to be seconded to the APO, on a cost-recovered basis, to assist APO investigators with passport fraud investigations and assist in the development of their skills, perform a liaison role and conduct complex passport fraud investigations.²⁸ Although the police

²⁶ ANAO Audit Report No.24 2007–08, *DIAC's Management of the Introduction of Biometric Technologies*, discusses the *Biometrics for Border Control* initiative.

²⁷ *Memorandum of Understanding between Australian Federal Police and Department of Foreign Affairs and Trade in relation to Outposted Federal Agents*, entered into on 21 July 2008.

²⁸ The AFP generally investigates passport fraud cases that are relevant to wider criminal activity.

officer is based at the APO's Sydney office, the APO considers the officer to be a national resource for all APO investigative officers to consult.

2.24 Both the AFP and APO commented positively on the arrangement, finding it to be of mutual benefit. In response to an ANAO suggestion, the agencies will review the cost-sharing arrangement, and consider a possible extension of the arrangement to other APO offices, at the expiration of the current MOU (in July 2012).

Customs and Border Protection and SmartGate

2.25 With thousands of Australian ePassport holders using SmartGate each day, cooperation with Customs and Border Protection is important to monitor the effectiveness of the ePassport in facilitating clearance across the border.²⁹

2.26 The APO and Customs and Border Protection have established an MOU to manage the exchange of PKI certificates, which are used to validate the authenticity of ePassports issued by APO and presented at the border. This MOU assigns responsibility to DFAT for developing and implementing reliable systems for distributing PKI certificates to Customs and Border Protection. This arrangement generally works well.³⁰

2.27 Where Customs and Border Protection experiences difficulty in reading a passport at the border, it contacts DFAT's Consular Emergency Centre (CEC) to confirm its validity. The contact is recorded in a daily log and brought to the attention of the APO. A small, but unknown number of ePassport holders are referred by Customs and Border Protection to the APO because the microchip fails to read at the border.³¹ However, the APO advised the ANAO that it invariably finds the microchip to be working and considers that the

²⁹ The ANAO is conducting a parallel audit of incoming passenger processing, which will include an examination of SmartGate.

³⁰ The ANAO identified one issue that caused inconvenience to a number of travellers, but did not compromise the ePassport's security. In July and August 2009, a PKI database anomaly prevented a number of 'M' series ePassports issued in April 2009 from being used by SmartGate and caused about 140 ePassport holders a day—approximately 4 per cent of those presenting at SmartGate—to be referred for manual processing. This issue was resolved for affected Australian ePassport holders on 28 August 2009.

³¹ Difficulties in reading a passport may occur for a number of reasons, including damage to the booklet, the microchip or the machine readable zone. The specific reason may not be recorded. The Consular Emergency Centre guidance currently provides for microchip reading errors at the border to be logged as a 'damaged' passport, rather than a read error on the microchip, meaning that data on the incidence of microchip-related errors is not readily accessible.

problem is more likely to relate to errors in operating the SmartGate ePassport reader.

2.28 To reduce the inconvenience to the passport holder, the ANAO suggested that the APO work with Customs and Border Protection to develop a joint strategy to better measure and manage this issue. In response, the APO and Customs and Border Protection agreed that a joint strategy would be beneficial, with the APO advising that it will seek to establish a joint working group to develop a strategy and jointly manage issues associated with ePassport usage at the border.

Arrangements for exchanging information

2.29 The APO and its stakeholders have an ongoing need to exchange information for identity verification purposes. Under the *Australian Passports Act 2005*, the APO may seek personal information to determine a person's eligibility for a passport and may disclose personal information to other agencies for a number of reasons.³²

2.30 To this end, the APO exchanges information with a number of federal and state agencies. For example, the APO:

- allows for the validity of passports to be checked through the Document Verification Service and can itself check the validity of identity documents such as birth, death and marriage certificates;
- is able to access an extract of DIAC's citizenship records;
- provides DIAC with updated extracts of the Passport Issue and Control System (PICS) to check passport records (although only a small number of DIAC officers have access and can only search by document number); and
- provides samples of genuine passports to other agencies and consults with them about the design of the booklet.

2.31 While the APO is authorised by the *Australian Passports Act 2005* to disclose information in prescribed circumstances for law enforcement purposes, no agencies have direct access to the APO's FR database or biometric

³² Sections 43 to 46 of the *Australian Passports Act 2005* provide that the APO may disclose information for law enforcement and family law matters or to comply with any law of the Commonwealth, subject to a ministerial determination.

templates. However, the APO promotes its FR capabilities as a resource to assist national law enforcement (see case study in Figure 2.1).

Figure 2.1

Case Study

Inter-agency cooperation in detecting identity crime

State-based police identified individuals suspected of committing identity fraud. A photograph of one suspect was sent to the APO for FR matching. The APO found that this individual had fraudulently obtained three genuine passports. Further investigation identified another individual who had conspired in the crime.

Source: ANAO analysis of APO data.

Intelligence sharing to combat passport fraud

2.32 The sharing of intelligence on passport fraud and methodologies helps agencies understand emerging risks and facilitates the investigation of specific cases. The ANAO's file reviews and interviews with key APO staff and stakeholders revealed that the APO engages with stakeholders in a number of activities to help combat passport and identity fraud. These activities include:

- cooperating with specific agencies, such as state roads and traffic authorities, on a case-by-case basis to undertake data-matching exercises to help identify incidences of identity fraud;
- fraud outreach, which involves briefing organisations such as financial institutions on the nature of passport fraud; and
- providing and receiving ad hoc operational intelligence from other agencies on passport fraud.

2.33 Nevertheless, the APO does not routinely prepare strategic intelligence briefs for stakeholders on passport fraud trends. However, the ANAO noted that some work has been undertaken by the APO in the past in this regard, and that during the audit the APO was seeking to reinvigorate its strategic intelligence capability.³³

Conclusion—Coordination and information sharing within Australia

2.34 The APO actively participates in relevant interdepartmental activities and its broader relationships with key stakeholders are collegial and

³³ For example, the APO wrote to the AFP, the Australian Security Intelligence Organisation, DIAC and Customs and Border Protection in mid-2011 seeking to enhance cooperation in this area.

cooperative. The APO promotes its FR capabilities as a resource to assist national law enforcement and has entered into a mutually beneficial arrangement with the AFP for the secondment of a police officer to its Sydney office. Overall, these arrangements indicate a mature and appropriate coordination approach with stakeholders.

2.35 Nevertheless, there are opportunities for the APO to strengthen its interaction with agencies, including through the development of a joint strategy with Customs and Border Protection to better quantify and manage the issue of ePassports that fail to read at the border. The APO and Customs and Border Protection agreed that a joint strategy would be beneficial, with the APO advising that it will seek to establish a joint working group to manage relevant border issues. At the time of the audit, the APO's strategic intelligence capability was limited, but the APO has flagged an intention to reinvigorate this capability.

3. Management and Operation of the Facial Recognition System

This chapter reviews the management and operation of the facial recognition (FR) technology used in the passport issuing process. In view of the sensitivities surrounding the FR system and the potential for passport fraud, some operational details have been omitted.

The passport issuing process—overview

3.1 The APO requires a robust passport issuing process to verify the identity of applicants and ensure that Australian passports are issued only to those who are entitled to hold them.³⁴ The current process has evolved over many years as the APO has sought to improve and strengthen it. The process involves a range of steps, as illustrated by Figure 3.1. Appendix 3 outlines these steps in more detail.

Figure 3.1

Passport issuing process



Source: ANAO analysis of APO data.

3.2 The introduction of the ePassport opened up possibilities for strengthening the passport issuing process, including the use of FR matching to reduce the incidence of passport fraud. The use of FR matching during the passport issuing process (highlighted in grey in Figure 3.1) is not an international requirement and Australia was one of the first countries to introduce it for this purpose. The APO's FR approach involves two elements:

- the automated identification of potential matches by its FR system (management of the FR system); and

³⁴ The *Report to the Council of Australian Governments on the elements of the National Identity Security Strategy*, April 2007, noted that secure enrolment is a prerequisite to building an identity security system of high integrity (p. 3).

- the subsequent consideration of those potential matches by an Eligibility Officer (operation of the FR system).

Management of the facial recognition system

Facial recognition matching process

3.3 FR systems are computer programs that analyse images of human faces for the purpose of comparing them to other faces. Typically, these programs take a facial image and measure certain characteristics, such as the distance between the eyes. These measurements are used to create a mathematical representation called a 'template'. The software then compares that template with other templates and produces a score that measures how similar the templates are to each other.

3.4 At the time ePassports were introduced in October 2005, the APO established a FR database containing templates for passport applications from the year 2000. Passport photographs from all passport applications since 2005 have been added to the database as part of the current passport issuing process.³⁵

3.5 As the FR check is but one of the 200 checks performed, the passport workflow has been designed so that it can be overridden (with the approval of the APO Senior Executive) should the FR system fail, to enable passport processing to continue. However, the APO has advised that all images would be checked once the system is restored, including any emergency passports issued by overseas posts.

Review of the facial recognition system

3.6 Three years after introducing FR into the passport issuing process, the APO engaged a contractor to review its operation. This review was completed in November 2008 and provided the APO with a timely and comprehensive baseline assessment of the system's operation.

3.7 The review concluded that the system was impressive in terms of its robustness, performance and scalability. However, the review also identified a range of factors with the potential to put the system at risk into the future, and

³⁵ At the time of the audit no photographs had been deleted from the database and therefore some passport holders who had renewed their passports had more than one image in the database.

made a number of short and long-term observations and recommendations to address these. These included:

- developing comprehensive system documentation;
- developing FR training programs for Eligibility Officers;
- establishing separate system environments for development, testing and production;
- using commercial off-the-shelf tools to undertake automated image cropping and image compliance assessments to improve the quality of images enrolled in the FR system; and
- introducing investigative tools to facilitate detailed facial image comparisons.

3.8 The APO largely accepted the recommendations and observations, but at the time of the audit fieldwork in 2011 most had not been implemented. The APO advised that implementation of some recommendations was impractical in the short term, and for others it had been delayed while a biometric service panel was put in place to supply the services required.³⁶

3.9 During the audit, the APO developed a FR Future Directions Plan (the Plan) to address outstanding recommendations. The Plan was approved by the APO Senior Executive in March 2012. Among other things, the Plan sets out objectives, potential business benefits and a risk rating for each identified activity. Importantly, it categorises activities for implementation in the short, medium and longer-term, with targets of June 2012, June 2013 and June 2015, respectively.

3.10 The development of the Plan is an important milestone in taking the recommendations and observations forward. However, delays in establishing the panel and developing the Plan means that some weaknesses will not be addressed until well after the desirable timeframes envisaged in 2008. Implementation of the Plan would benefit from ongoing active management oversight and periodic progress reviews to ensure that key issues are addressed in a timely manner.

³⁶ The panel was established in September 2011. The APO advised that the panel approach was initiated once it became evident that the cost of implementing most recommendations would exceed the \$80 000 threshold in the Commonwealth Procurement Guidelines and therefore involve lengthy public tender processes. The APO also advised that legal negotiations with suppliers delayed publication of the panel.

System documentation and expertise

3.11 It is important that the operation and use of the FR system be adequately documented to establish a system baseline and to assist system review and development. However, the 2008 review found a lack of adequate documentation on the system.

3.12 While this issue had not been resolved at the time of the audit fieldwork, the APO has since engaged a contractor from its newly established biometrics panel to develop documentation by June 2012.

3.13 Similarly, the 2008 review found that system maintenance and support relied on an individual officer that placed the operation of the system at risk. Although this weakness had also been recognised by the APO as early as 2005–06, it had not been overcome at the time of the audit fieldwork. The APO has since advised that responsibility for the IT components of the passport systems and processes (including staffing) has now been transferred to DFAT's Information Management Division. The APO has undertaken to work with that division to develop and implement a long-term solution. The FR system documentation developed during the audit should also help to mitigate this risk.

Testing algorithms and setting thresholds

3.14 The APO uses a commercially supplied biometric algorithm to convert passport photographs into templates and enable its FR matching system to compare the applicant's template to all other templates in the database (known as 'one-to-many matching').³⁷ In determining the commercial supplier, the APO took into account the match rate (using known image pairs)³⁸ and the search/match speed of the algorithm.³⁹

3.15 Companies developing biometric algorithms seek to continuously improve their algorithms and sell the new versions to users. The APO's FR

³⁷ The system is also used for one-to-one matching (to verify that the person renewing the passport is the same person who originally applied for it) and one-to-few (to determine if the applicant is on a watchlist).

³⁸ Known image pairs (also known as matched pairs or true pairs) involve two images known to be of the same person. Known pairs are used to test the match rate and speed of FR matching systems.

³⁹ Speed is important to enable matching to occur during real-time application processing. The FR system is required to process 6000 to 8000 applications within a 10-hour period each day to enable the APO to meet its passport application processing time. The APO advises that the FR matching arrangement therefore needs to process each request in about two seconds. This is also considered to provide a buffer to manage database growth.

system is currently using its third new algorithm since 2005 and, at the time of the audit, the APO was testing another version. The APO advised that testing currently involves comparing the effectiveness of the new and old algorithms against some 1.2 million known image pairs. The APO also advised that following testing, a case for introducing the new algorithm is put to the APO management for review and decision.

3.16 While this appears to be a sound approach, the APO could not locate the relevant documentation for its test methodology⁴⁰, the test outcomes for the current and previous algorithms, and the recommendations put to APO management for decision. Therefore the ANAO could not assess whether the decisions to implement the new algorithms were soundly based. The APO subsequently advised the ANAO that the test methodology will be documented, and that the algorithm vendor will be engaged to conduct a health check of the system and to provide advice on improving the FR system's performance, in the first half of 2012.

Matching thresholds

3.17 The FR system compares the applicant's template to other relevant templates in the FR database using filtering (known as 'binning'). The system displays up to 10 facial matches in an FR gallery based on the matching threshold set by the APO. The gallery is reviewed by the APO's Eligibility Officers.

3.18 Setting the threshold too low will increase the number of potential matches returned to the gallery and increase the time taken by Eligibility Officers to review the photographs and hence impact on workload and resources required to process the applications. Setting the threshold too high may exclude some true matches and therefore reduce the likelihood of identifying passport fraud.

3.19 While the APO has adjusted the threshold since FR matching was introduced in 2005, the APO could not locate the relevant documentation that would enable the ANAO to review the business case for selecting the current threshold. However, the 2008 review noted that the current threshold was relatively high and could lead to an unacceptably high false rejection rate (where the system fails to identify someone already enrolled). Furthermore,

⁴⁰ The test methodology should comprise test criteria, a test plan, test data, expected test results, and an analysis of the actual results against the expected results.

while some work to identify false rejection rates and false acceptance rates was undertaken at the time the FR system was introduced⁴¹, little work has been undertaken since.⁴² Understanding these rates is important as they help to identify the risks associated with key system settings, including the threshold and gallery size, and the filtering used. More importantly, they are an important measure of whether the system is working as intended.

3.20 In response to these findings, the APO advised that as part of the 2012 review, the algorithm vendor will assess the FR system's false rejection and acceptance rates and provide advice on the threshold and filtering settings. In addition to this work, to help assess the risks associated with particular system settings and optimise system performance, it will be important for the APO to develop and document a mechanism for ongoing assessment and adjustment of the threshold, including ongoing monitoring of false rejection and acceptance rates. This approach will better equip the APO Senior Executive to weigh future trade-offs between workload and the probability of fraud detection. Documenting management's consideration of future proposed changes to the system settings will also strengthen accountability and facilitate future review.

Facial recognition system backup and test system environment

3.21 At the time of the audit there were separate system environments for live production and system testing purposes. The 2008 review recommended that a third environment be available for system development purposes. In addition, the APO's IT disaster recovery arrangements did not cover the FR system so that, should the production system break down and the backup data centre be required to operate, there would be no FR functionality available. In response, the APO advised that funding for the third environment had been obtained and that both it and a disaster recovery arrangement for the FR system would be operational by June 2012.

⁴¹ The false rejection rate is the probability of the FR system failing to return a match for an applicant already enrolled. Conversely, the false acceptance rate is the probability of the system incorrectly returning a match against an applicant who is not already enrolled.

⁴² In late 2009 the APO developed a proposal to engage a contractor to identify false rejection rates and their impact on the threshold, but this was not pursued pending the establishment of the biometric service panel.

Pending/watchlist database

3.22 The APO is alert to the risk that two or more applications by the same person could be lodged and processed simultaneously, prior to the facial image being enrolled in its FR repository. To mitigate this risk it has established a 'pending database' that holds current applications and those that have been recently processed. The pending database also includes a 'watchlist' that contains information on 'persons of interest'.⁴³ As each applicant's image is checked against the main FR system as part of the eligibility process, it is also checked against the pending database.

3.23 The current passport issuing system does not incorporate the pending database check in the end-to-end process workflow. This means that a match resulting from the pending database check will not automatically stop downstream processing, but requires manual intervention from staff to stop the printing of the passport and to refer the case to the appropriate area for investigation. The risk is that fraudulent applications may pass through the workflow for printing and issuing before manual intervention occurs. This would require the issued passport to be revoked and recalled.

3.24 In addition, at the time of the audit, there was limited documentation on the pending database and no clearly documented policy of who would qualify for inclusion on the watchlist.

3.25 These issues have been identified in the Future Directions Plan. The Plan provides for the integration of the pending database into the workflow process, and for the development of a policy, process and procedure for establishing and maintaining a watchlist to manage sensitive cases, by June 2013.

⁴³ Persons of interest may include persons who are 'wanted' by authorities and those who may have held or sought to obtain a fraudulent passport in the past.



Personalisation and printing of Australian ePassports, including microchip encoding.

Photo: DFAT

Image quality

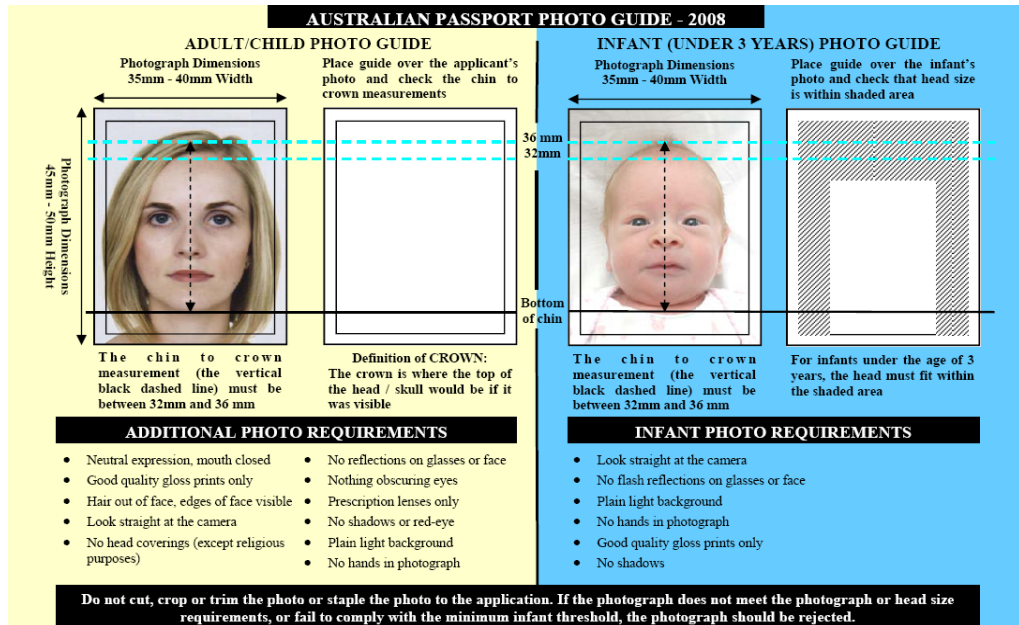
3.26 Australia has adopted the ICAO/ISO recommended standards⁴⁴ for its passport photographs. A failure to comply with these standards would affect the performance of the APO's FR matching system, and would impact on the effectiveness of FR matching at Australian and international border controls.⁴⁵ Currently the approach adopted by the APO uses people to visually inspect and assess applicants' photographs against the ICAO standards (summarised in Figure 3.2) during both the interview and data capture processes (outlined at Appendix 3). The APO considers that its approach meets all ICAO/ISO requirements in this regard.

⁴⁴ International Civil Aviation Organization, *Machine Readable Travel Documents*, Document 9303, and International Organization for Standardization/International Electrotechnical Commission 19794-5. The ICAO facial image standard is based around creating a repeatable facial expression for the purposes of consistent matching performance and interoperability with FR systems. The more facial images are presented in the same way (e.g., eyes open, mouth closed) the better the FR systems will perform.

⁴⁵ Customs and Border Protection confirmed that the quality of images stored on the Australian ePassport microchip does impact on the effectiveness of FR matching used by SmartGate. However, it advised that the number of FR referrals attributable to image quality remains relatively small and within tolerable levels. It noted that there continues to be a steady improvement in the efficiency of biometric algorithms that will, over time, reduce the impact of poor image quality.

Figure 3.2

Australian passport photograph guidance



Australian Passport Photo Guide 2008. The APO uses people to visually inspect applicants' photographs against ICAO standards. More detailed guidance for applicants and photographers is on the APO's website <<https://www.passports.gov.au/Web/index.aspx>.>

Source: Australian Passport Office.

3.27 It is also possible to assess applicants' photographs using automated image quality checking software. While it is not an ICAO/ISO requirement to use this software, and there is always margin for error in using a software solution, the use of automated checking has the potential to yield efficiency gains and scrutinise images more consistently and objectively, and in much greater detail than a visual inspection by a person.

3.28 The software also has the potential to improve image quality and the effectiveness of FR technology during application processing and at the border, however, it is not practical to implement in Australia at this time. Implementation would involve both additional cost and a significant change to the APO's passport issuing process—that is, from the current method of

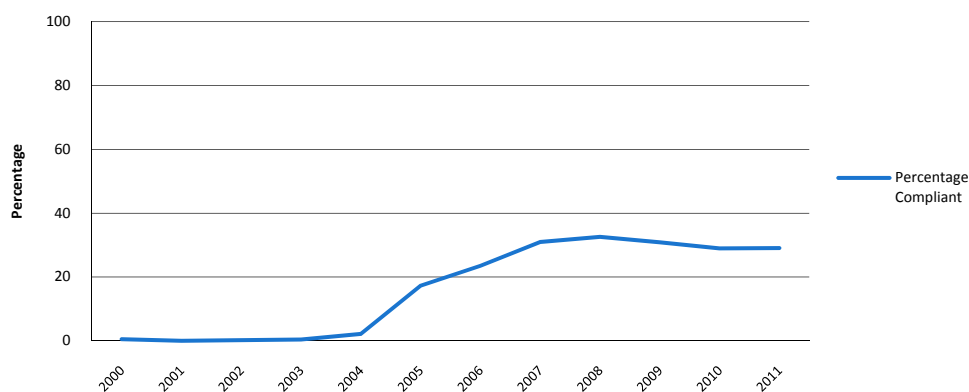
scanning applicants' photographs, to the live capture of digital images.⁴⁶ These issues are explored below.

Potential use of automated image quality checking software

3.29 The 2008 review examined a sample of 11 000 images enrolled between 2000–2008 using non-mandatory automated image quality checking software and found that nearly 90 per cent would not have complied with the ICAO standard had the software been used. However, the review found that the compliance rate had increased from less than 1 per cent in 2000 to almost 33 per cent in 2008.⁴⁷ Data recently provided by the APO suggests that the compliance rate has remained at about 30 per cent since that time (see Figure 3.3).

Figure 3.3

Percentage of images complying with standards as tested by automated image software



Note: The APO advised that images captured prior to 2005 were not captured using the ICAO standard as FR was not used at that time.

Source: Australian Passport Office (including 2008 review of facial recognition).

3.30 Common reasons for non-compliance when the non-mandatory software was used included poor image resolution and poor face positioning and dimensions, which were affected by the APO's processes for capturing

⁴⁶ Live capture would involve the applicant's photograph being taken by the APO or its agent (Australia Post) during application processing.

⁴⁷ Since the introduction of ePassports the APO has actively engaged with the photographic industry to improve the quality of submitted photographs and updated its general photographic guidance. During the ANAO's visits to APO state offices, staff confirmed that image quality has improved over the years.

and manually cropping photographs.⁴⁸ The review recommended that the APO employ commercial off-the-shelf tools to undertake automated image cropping and image compliance assessments to improve the quality of images enrolled in the FR system.

3.31 At the time of this audit the APO had not acquired the recommended commercial off-the-shelf software and integrated it into its workflow, although it had investigated its functionality and availability. It advised that automated cropping software would not always correctly crop the photograph and that automated image compliance software would significantly disrupt the passport issuing process as the majority of photographs currently accepted would be rejected. The APO advised that rejecting photographs would inconvenience the applicant, adversely impact on the photographic industry and require additional APO resources to administer.

3.32 Since the 2008 review, the APO has been collecting data to enable it to analyse the quality of images enrolled in the passports database.⁴⁹ The APO advised that, while the software it is using to collect this data suggested that the compliance rate remained at about 30 per cent (see Figure 3.3 above), it had concerns about whether the software was fully reliable. It expected that detailed analysis will assist in determining the compliance rate, and how the facial image capture process can be further improved. The APO advised that automated checking will be explored as part of its Future Directions Plan, but that it could not be introduced unless a live capture facility is also implemented.

Live capture

3.33 The APO considers that the best way of improving image quality is to change from its current approach of scanning photographs submitted by applicants, to the live capture of digital images. Live capture has a number of significant advantages as it would:

- be more efficient, removing the need to scan and crop all photographs;

⁴⁸ Capture involves passport applicants providing photographs which are then scanned into APO systems. The scanned images are then cropped (trimmed) manually by APO staff to position them. The cropped image is then used for FR matching. APO advised that the facial images originally enrolled into the FR system in 2005 were automatically cropped as part of the enrolment process. However, the automatic cropping process did not crop all images correctly and over the last two years it has manually re-cropped all the pre-2005 images and re-enrolled them into the FR system.

⁴⁹ Although the APO has not introduced image compliance software into its workflow, it has an assessment algorithm that enables it to test the quality of the images against the ICAO automated software standard.

- enable the use of automated image compliance software;
- substantially improve image quality; and
- strengthen the identity verification process.

3.34 The APO advised that it has considered a proposal for the live capture of images, but considers that it would be too expensive to implement at this point. However, it has identified a scoping study on live capture in its Future Directions Plan and advised that it will pilot live capture as part of the Passport Redevelopment Program with wider deployment to be considered by APO/DFAT management.

Conclusion—Management of the facial recognition system

3.35 The FR system is one of a number of checks in the passport issuing process aimed at reducing the incidence of identity fraud. A timely review of the system was undertaken in 2008. However, most review recommendations, including the development of key system documentation and reducing reliance on an individual for system maintenance and support, had not been implemented at the time of the audit fieldwork in 2011. The APO subsequently engaged a contractor to document FR systems and developed a strategy to overcome this potential single point of failure. While it also developed a FR Future Directions Plan to take other outstanding issues forward, implementation of the Plan would benefit from ongoing active management oversight and periodic progress review, to ensure that key issues are addressed in a timely manner.

3.36 The APO has updated the FR system for new algorithms but was unable to locate documentation of its test methodology and outcomes, including the adjustment of the threshold, and their consideration by management. Therefore, the ANAO could not assess whether the decisions to implement the new algorithms and adjust thresholds were soundly based.

3.37 In response to these findings, the APO advised that its test methodology will be documented and a health check of the FR system undertaken in the first half of 2012, which will cover false rejection and acceptance rate analysis and the threshold and filtering settings. It will also be important for the APO to develop and document a mechanism for ongoing assessment and adjustment of the FR system settings and monitoring of outcomes, to help optimise system performance. This approach will better equip the APO Senior Executive to weigh future trade-offs between workload and the probability of fraud detection. Documenting management's

consideration of future proposed changes to the system settings would also strengthen accountability and facilitate future review.

3.38 The APO uses people to visually inspect and verify that submitted photographs meet ICAO standards, and considers that it meets all international requirements in this regard. While automated image quality checking software has the potential to improve image quality and therefore the effectiveness of FR technology during application processing and at the border, it is not an international requirement nor is it practical to implement at this time. The APO intends to pilot live capture which would facilitate the use of automated image checking software.

Recommendation No. 1

3.39 To strengthen the management of its facial recognition system, the ANAO recommends that the APO:

- periodically review progress in addressing the outstanding observations and recommendations identified in 2008 so that key issues are dealt with in a timely manner; and
- develop and document a mechanism for the ongoing assessment and adjustment of the facial recognition system settings and document management's consideration of future proposed changes to those settings.

DFAT response

3.40 DFAT agrees with this recommendation. DFAT has developed a Future Directions Plan and established a Biometrics Goods and Services Panel to take forward the outstanding issues identified in the 2008 review of its facial recognition system.

Operation of the facial recognition system

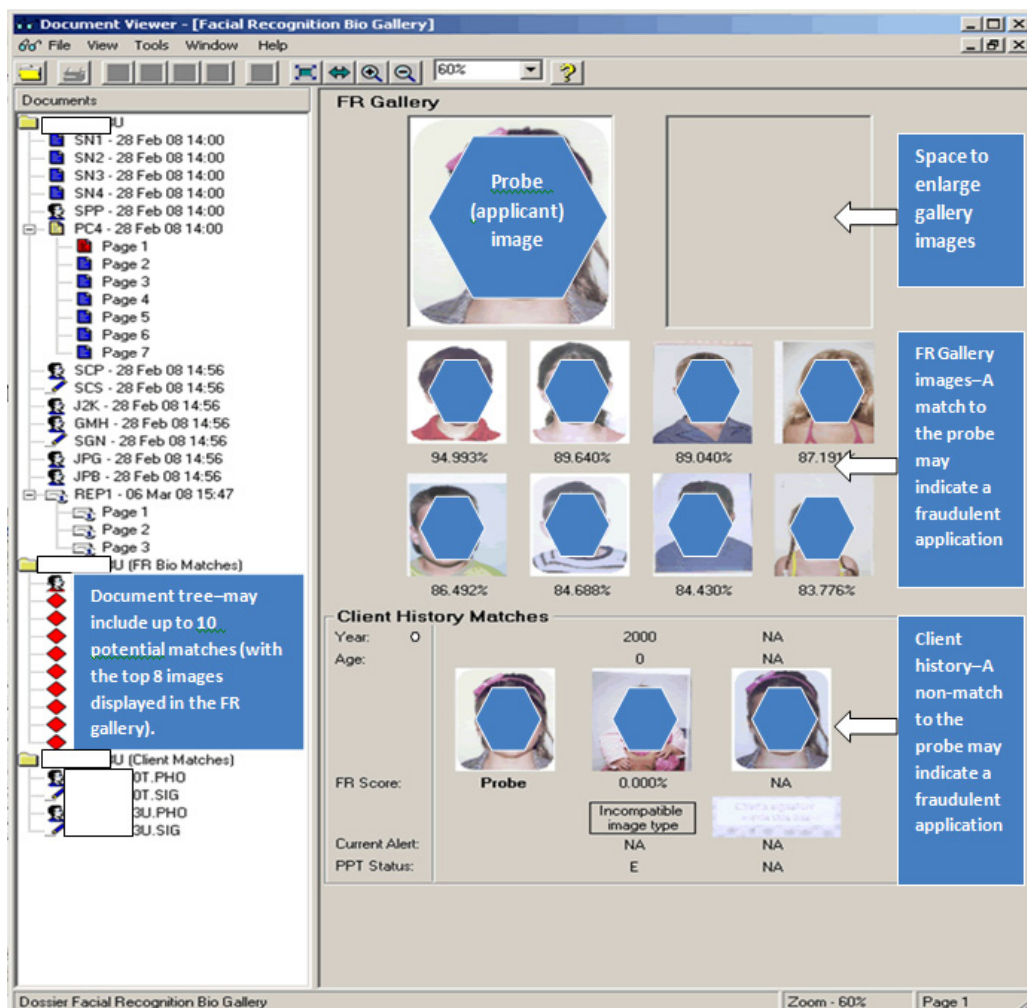
3.41 Once potential matches have been identified by the automated FR matching system, APO Eligibility Officers are required to review them to determine whether any require more detailed investigation. To facilitate this process, potential matches should be presented in an efficient and effective display, and Eligibility Officers should have access to appropriate and timely training, and clear, relevant and up-to-date guidance.

Reviewing potential matches in the gallery

3.42 Potential FR matches are displayed in a gallery for Eligibility Officers to review. The APO has revised the gallery layout once since FR matching was introduced in 2005. The revision, which was made in early 2008, resulted in the current presentation shown in Figure 3.4.

Figure 3.4

Facial recognition gallery showing potential matches



Source: ANAO, based on APO gallery image.

3.43 The revised layout was generally considered by Eligibility Officers to be an improvement. For example, it allowed gallery images to be compared side-by-side with the applicant's photograph (known as the 'probe'). However, the 2008 review noted that the revised layout remained difficult for

Eligibility Officers to use efficiently and effectively. In particular, it found the images were very small and that it would be difficult to visually compare these images against the probe image. It recommended that the display be reviewed to improve its usability and effectiveness.

3.44 The ANAO observed Eligibility Officers review gallery images during its visits to APO state offices and noted different approaches. Some staff routinely elevated each gallery image next to the probe to enlarge it, while others compared the probe to the smaller images, elevating them only occasionally. In some cases, staff used a known workaround and copied gallery images to a word processing application to enable further enlargement and better comparison with the probe.

3.45 In response to these issues, the APO advised that it expects to test and deploy an enhanced FR gallery by June 2012 that will enable Eligibility Officers to further enlarge selected images in the gallery and compare them side by side against the probe.

Reviewing photos nine and ten in the 'document tree'

3.46 The ANAO noted that where the FR system returns nine or ten matching images, only the top eight are displayed in the gallery, with up to two more listed in the 'document tree' (see red diamonds in Figure 3.4). APO's expectation is that these additional images will be viewed by the Eligibility Officer before application processing continues, however, there is no system function that ensures that these images are viewed, and no log of whether it occurs. The APO advised that its planned 2012 gallery enhancements will allow up to 10 images to be displayed in the gallery.

Facial recognition training and guidance for Eligibility Officers

Training

3.47 Initial training for Eligibility Officers involves a five-day training course that covers a range of issues including their role, the legislative framework and IT systems. The course includes an overview of passport fraud and limited (about one hour) FR training. The latter includes a self-paced Passport Electronic Training module that takes staff about 20 minutes to complete. While a one-off FR refresher training course was undertaken in 2009, ongoing FR refresher training is not mandatory, nor is a record kept of those who undertake it.

3.48 In October 2010, the APO engaged a contractor to review its FR training practices. The review generally found its training materials to be basic and, in

some cases, out of date. Among other things, it noted that competency assessments were not undertaken to measure how accurately Eligibility Officers could detect fraud attempts and that Eligibility Officers did not use a systematic approach to resolve difficult cases.

3.49 The APO advised that, in response to the review, it was updating its FR training material, and developing a medium to long-term training strategy, to be completed by June 2012. This will include a framework and policy on mandatory refresher training and assessments for staff involved in FR decision-making. The APO also advised that it has now put in place a system to automatically record the completion of training.

Guidance on escalating possible fraud cases

3.50 Where Eligibility Officers suspect fraud they are required to discuss the matter with a more senior Eligibility Officer and/or refer it to the Passport Fraud Section for investigation.⁵⁰ However, the APO's FR guidance lacked substantial advice and discussion on the issues that Eligibility Officers should consider in deciding on the action required when identity fraud is suspected. In addition, some of the guidance was out of date.

3.51 The lack of formal processes and criteria for escalating possible fraud cases was identified by the 2008 review noted above. While the APO accepted those findings, it had not adequately addressed this issue at the time of this audit. The ongoing lack of guidance in this area, combined with weaknesses in existing FR training, creates a risk that suspected identity fraud will not be consistently dealt with by Eligibility Officers and escalated as required.

3.52 In response to these findings, the APO undertook to update its FR guidance material as part of its training strategy. In addition, it advised that work it had underway to establish an Identity Resolution Unit in Canberra for managing difficult identities, and the automation of fraud referrals to the Passport Fraud Section as part of the Passport Redevelopment Program, will strengthen the identity verification process and improve its fraud detection capability.

⁵⁰ Eligibility Officers are graded A, B and C, depending on their level of experience. Level C officers assess more difficult cases and supervise A and B officers.

The human factor

3.53 While the FR system generates a suite of potential matches, judgements about whether any of these might be a 'true' match relies on the assessments made by Eligibility Officers. Although most people are generally good at recognising familiar faces regardless of facial expression, lighting and other variables such as hair and glasses, decisions about matching unfamiliar faces often result in error. Research has demonstrated that individuals differ substantially in their ability to match unfamiliar faces, with some likely to be naturally better than others.

3.54 The APO is aware of this issue and is funding and actively collaborating with external researchers to improve the performance of Eligibility Officers in matching faces.⁵¹ Preliminary findings suggest that neither Eligibility Officers nor APO management have a clear idea of how well (or poorly) they are performing this task. In addition, preliminary testing of trained Eligibility Officers found that their matching performance was equivalent to control participants, which suggests that the APO's FR training has been ineffective. More appropriate training (for example, involving the provision of feedback) is considered to have significant potential to improve performance.

3.55 The APO advised that, as a part of its training strategy, it intends to continually update the training material based on the outcome of this research.

Conclusion—Operation of the facial recognition system

3.56 The FR gallery user interface has been revised since its introduction in 2005 but, at the time of the audit fieldwork, remained difficult for Eligibility Officers to use efficiently and effectively. To overcome these issues the APO will test and deploy an enhanced FR gallery in the first half of 2012.

3.57 Appropriate and up-to-date training and guidance material is important to support staff involved in FR matching. However, weaknesses in both areas were apparent at the time of the audit. In particular, there was

⁵¹ The APO is partially funding a three-year research project by the University of New South Wales which is seeking to: develop training procedures to increase operators ability to detect fraud; investigate how aspects of task presentation affect performance in unfamiliar facial comparison tasks; develop tests to predict the ability of operators to detect identity fraud in passport applications; and develop digital image manipulation tools which could be used to assist fraud detection experts when comparing facial images. The APO is also involved in a collaborative biometrics research program being undertaken by the Defence Science and Technology Organisation.

limited coverage of FR in the Eligibility Officer training course and while some refresher training had been undertaken in 2009, ongoing refresher training was not mandatory, nor was a record kept of those who undertook it. In addition, the FR guidance lacked substantial advice and discussion, and some material was out of date.

3.58 During the audit the APO took steps to overcome these weaknesses. In particular, it advised that it will update its FR training and guidance material, and develop a medium to long-term training strategy to address its training needs by June 2012. In addition, it will consider introducing periodic mandatory training and assessments for staff involved in FR decision-making, and advised that it has now put in place a system to automatically record the completion of training modules. The APO is also funding research work that should help to improve the performance of Eligibility Officers in matching faces and provide useful information on how to optimise their training.

4. The Impact of Facial Recognition Matching on Passport Fraud

This chapter examines the changing nature and incidence of passport fraud and the impact that the introduction of facial recognition (FR) matching into the passport issuing process has had in detecting that fraud. In view of the potential for passport fraud, some details on the nature of that fraud have been omitted.

The nature of passport fraud

4.1 Australian passports are regarded internationally as high-quality identity documents. In addition to their primary purpose of facilitating international travel, passports provide personal identification for people seeking access to a range of government and non-government services and benefits and are used to facilitate everyday transactions.⁵² However, if lost, stolen or otherwise fraudulently obtained, passports can be used by fraudsters to establish false identities and facilitate financial crime or other crime such as people smuggling or terrorist acts.

4.2 Against this background it is important that the identity of applicants is adequately checked by the APO to prevent passports being fraudulently obtained. The introduction of FR technology into the passport issuing process in 2005 sought to strengthen the integrity of passports in this regard.

The changing nature of passport fraud

4.3 Fraud against Australian passports may involve a range of offences, including:

- making false or misleading statements in a passport application;
- producing false or misleading documents in support of an application;
- improper use or possession of a passport;
- selling, damaging, altering or dishonestly obtaining a passport; and

⁵² Audit Report No.29 2009–10, *Attorney-General's Department Arrangements for the National Identity Security Strategy*, (Appendix 3), notes that the Australian passport is the most commonly accepted proof-of-identity document used by various Australian, state and territory government agencies when enrolling individuals for services.

- failing to report a lost or stolen passport.⁵³

4.4 The introduction of ePassports in 2005, together with the continuing enhancement of booklet security features, has been instrumental in shifting the focus of fraudsters from attempts at altering the passport document, to the inappropriate use of genuine documents. Emerging trends in passport fraud are outlined in Figure 4.1.

⁵³ A full list of offences relating to Australian travel documents is set out in Division 4 of the *Australian Passports Act 2005*.

Figure 4.1

Key emerging passport fraud trends

‘Available identity’ or ‘vulnerable identity’ fraud

A fraudster obtains another person’s proof-of-identity documents either with or without that person’s consent and applies for the issue of a genuine passport in that person’s name, but using their own photograph.

The victim may be, for example, mentally ill, disabled or a remote resident who the fraudster believes is unlikely to travel internationally (hence the term ‘available identity’).

ANAO comment:

- This fraud is unlikely to be detected by the APO at the time of passport issue unless the fraudster has already been issued with a passport in his/her own name or another name. In this latter case the FR matching technology used by the APO may identify the passport previously issued.

Imposter fraud

Involves the use of a valid, unaltered Australian passport to enter Australia unlawfully. For example, an Australian citizen departs Australia using their Australian passport which is then lost, stolen or sold.* The passport is used by an imposter to enter Australia unlawfully. The imposter may have a family resemblance to the owner or may alter their appearance to resemble the owner, enabling them to pass face-to-passport identification at the border.

The offence may be facilitated by the Australian citizen delaying reporting the passport lost or stolen until the imposter has entered Australia.

* Alternatively the passport is carried overseas by a third person or simply posted overseas.

ANAO comment:

- Imposter fraud of this kind is not possible for the APO to detect at the time of passport issuing.
- The passport is genuine and has not been altered and therefore is unlikely to attract particular attention at the border.
- It is not known how many imposters successfully make it through the border.
- While the introduction of compulsory validation of ePassports at the border using the FR capability of SmartGate would increase the assurance that the person presenting the passport is the legitimate owner, Customs and Border Protection advised that there would be practical difficulties in implementing such an arrangement.⁵⁴

Source: ANAO analysis of APO documents and discussions with APO staff and other stakeholders.

The incidence of passport fraud

4.5 According to information supplied by the APO during this audit, the number of new passport fraud cases detected by it and other agencies increased from 178 in 2003–04 to 849 in 2010–11 (see Figure 4.2 below).

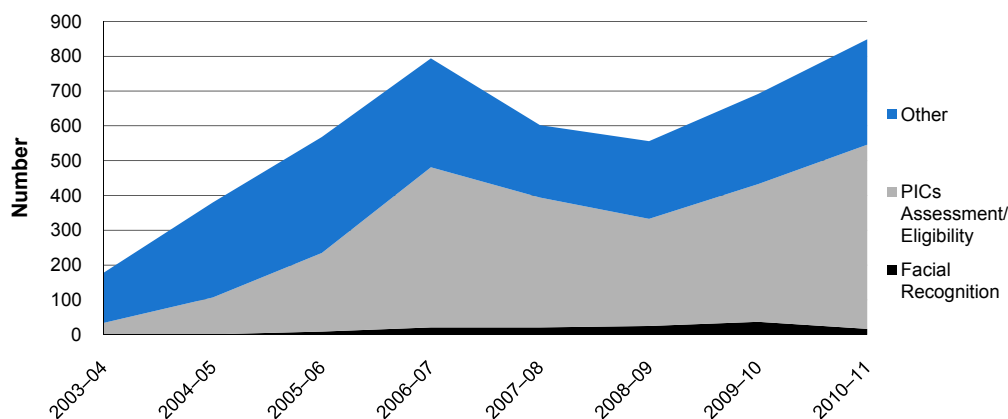
⁵⁴ Customs and Border Protection agreed that the introduction of compulsory validation of ePassports at the border using the FR capability of SmartGate would increase the assurance that the person presenting the passport is the legitimate owner. However, it advised that a number of constraints in the use of SmartGate, such as the limited capacity of SmartGate and its age and height restrictions, would make such a policy impossible to implement and enforce. It considers that a combination of SmartGate, the rollout of ePassport readers to all manual processing points at the eight international airports, ongoing training for officers performing face-to-passport checks, and improvements in intelligence sharing between government agencies around identity-related frauds will all assist in mitigating this risk.

4.6 The number of fraud cases shown in Figure 4.2 exceeds those reported in DFAT's Annual Report by between 0.5 per cent and 26 per cent, depending on the year. The APO attributes these differences to its overly complex, but limited, case management database from which it is problematic to extract data. This discrepancy weakens the assurance that the incidence of passport fraud is being carefully monitored and accurately reported.

4.7 The APO advised that its new case management system ('eCase') being developed as part of the Passport Redevelopment Program will enable the accurate recording of fraud statistics, provide the ability to extract statistics on the incidence of fraud against particular passport series, and facilitate fraud research. It also advised that an interim case management database solution that was implemented in February 2012 will enhance reporting capabilities in a number of areas and will be a major improvement over the current system.

Figure 4.2

New fraud cases (by detection method)



Source: ANAO analysis of APO data.

Notes: 'Other' detection methods include up to 12 other categories such as fraud detected at the border, by other agencies such as the AFP and information from informers.

APO considers that the number of fraud cases detected by its FR technology is understated. This issue is discussed further below.

4.8 The APO attributes the increase in the number of fraud cases to the increasing number of passports being issued (up from 1.1 million in 2003-04 to

1.8 million in 2010–11)⁵⁵ and to its increased investigative capability, rather than to an increase in the rate or incidence of fraud per se.

4.9 The ANAO has confirmed that the APO substantially increased its passport fraud detection and investigative capacity over this period and at the same time continued to strengthen its identity verification arrangements for applicants. The APO estimates that some 40 per cent of fraud is detected pre-issue, with the majority detected post-issue. However, accurate information on the percentage detected pre and post-issue over time was not available at the time of the audit. This information could provide a useful performance indicator for the effectiveness of fraud prevention measures that are employed during the passport issuing process. The APO advised that the interim case management database solution that was implemented in February 2012 will enhance reporting capabilities in this regard.

Investigating suspected fraud

4.10 Suspected identity fraud is sometimes detected by the FR technology used during the passport issuing process. Where Eligibility Officers suspect that an applicant may already have a passport in a different name, they are required to refer the application to fraud investigators in a specialist APO fraud unit (the Passport Fraud Section). This unit has staff in Canberra and four state offices.⁵⁶

4.11 The 2008 review of the FR system recommended that the APO introduce sophisticated specialist tools to enable more detailed facial image comparisons to be made by fraud investigators when reviewing suspected cases.

4.12 To this end, in 2009 the APO commenced trialling special software—*Expertise Pro*—to facilitate the comparison of potentially matching images. The software enables images to be imported into a gallery, enlarged, aligned and overlaid to facilitate the comparison of key facial features. At the time of this audit, the use of this software was restricted to particular fraud

⁵⁵ Over the same period the total number of passports in circulation increased from 7.9 million to 11 million.

⁵⁶ Most fraud investigations are handled by the APO's specialist fraud unit. The fraud unit is required to refer instances of potential serious or complex fraud offences to the AFP in accordance with the *Commonwealth Fraud Control Guidelines* (March 2011). Where appropriate, cases are referred to the Commonwealth Director of Public Prosecutions.

staff in Canberra⁵⁷ and was generally well-regarded by those staff. While technical issues have delayed the rollout of the software to state office fraud investigators, the APO advises that this will occur by June 2012.

4.13 At the time of the audit, the APO was also seeking to establish an Identity Resolution Unit in Canberra that is expected to become a centre of expertise for facial comparisons.⁵⁸ The ANAO sees advantages in identifying and concentrating expertise in one location and notes that this should be useful in assisting eligibility staff to resolve contentious FR issues.

Document examination

4.14 The APO maintains a document examination capability that, among other things, forensically examines and reports on passports found to have been fraudulently altered post-issue. The ANAO examined six recent reports, including one on the first two fraudulently altered 'N' series passports identified.⁵⁹ Importantly, the report analysed the methodology used by the fraudsters, identified lessons to be considered in the development of the proposed 'P' series⁶⁰ and recommended that the report be provided to key stakeholders for their information.

The impact of facial recognition matching on passport fraud

4.15 The key reason for introducing FR matching technology into the passport issuing process was to improve identity verification and reduce fraud.

4.16 The ANAO's interviews with APO staff and key stakeholders, together with its file reviews, confirmed that the use of FR in the passport issuing process has been successful in detecting many cases of identity fraud that would not otherwise have been detected. In one case, a FR match led to an

⁵⁷ State fraud investigators are able to send images to Canberra for review.

⁵⁸ The APO advised that there is increasing evidence that some people are inherently good at facial recognition and that training may have minimal impact on those who are not. This issue is currently being examined as part of a research project that is underway at the University of NSW.

⁵⁹ The 'N' series passport was introduced in May 2009. The report noted that the two 'N' series passports had been stolen and the biographical data pages replaced with counterfeit pages. The microchips showed the legitimate bearer's details and had not been altered or disabled. However, the microchips would not have been readable at the border due to errors in the machine readable zone.

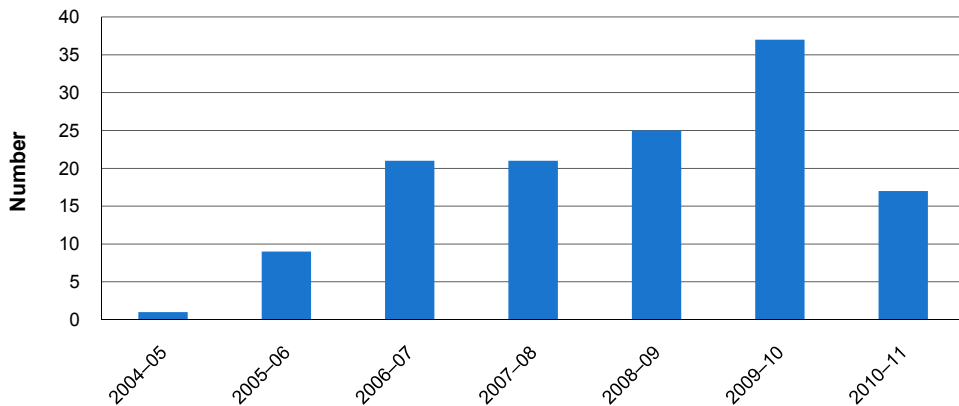
⁶⁰ The 'P' series is expected to be introduced in 2014.

investigation that revealed 15 other fraudulently obtained passports. In some cases, subsequent investigations also revealed fraud involving foreign passports, driver's licences, firearms and financial matters, including fraudulent Centrelink payments.

4.17 The number of passport fraud cases *recorded* by the APO as being detected through FR matching averaged about 22 a year over the period 2005–06 to 2010–11 (see Figure 4.3).

Figure 4.3

Fraud cases *recorded* as being detected by FR matching



Source: ANAO analysis of APO data.

4.18 However, these figures are understated by an unknown amount due to incorrect recording of the detection method in the passports database for some FR matches. This impairs the APO's ability to accurately quantify the success of the FR system in detecting passport fraud. Such information would be particularly useful in identifying the cost-effectiveness of the current technology and in justifying any potential enhancements to that technology. The APO advised that these weaknesses will be addressed by the interim case management database solution that was implemented in February 2012, and by ongoing training for staff on that system.

Conclusion—The impact of facial recognition on passport fraud

4.19 The introduction of ePassports in 2005 has helped shift the focus of fraudsters from attempting to alter passport booklets to attempting to fraudulently obtain genuine passports. While there has been a substantial increase in the number of passport fraud cases detected since 2003–04, the APO attributes this to the growing number of passports issued and to its greater investigative capability.

4.20 At the time of the audit there were difficulties in extracting accurate data from APO systems on the nature and incidence of passport fraud, which weakens the assurance that it has been being carefully monitored and accurately reported. In addition, while FR matching has detected many cases of identity fraud that would not otherwise have been detected, the incorrect recording of the detection method for some FR matches impairs the APO's ability to accurately quantify the success of the FR system in detecting fraud.

4.21 The APO advised that the new case management system ('eCase') being developed as part of the Passport Redevelopment Program, and an interim solution that was implemented in February 2012, will enable the accurate recording and extraction of fraud statistics.

5. Securing the ePassport's Microchip and Protecting Privacy

This chapter examines whether the ePassport's microchip has adequate security to protect personal data and provide assurance to border officials about the passport's validity. In addition, it assesses the effectiveness of the APO's approach to monitoring and protecting the privacy of passport holders' information.

Securing and verifying ePassport data

5.1 The ePassport's contactless RFID microchip uses a specific radio frequency to communicate over a limited range with ePassport readers. The intention is that the microchip be readable by all border officials in accordance with international standards. Nevertheless, appropriate security mechanisms, such as encryption systems, are necessary to prevent unauthorised access to, and potential manipulation of, ePassport data and communications between the ePassport and the passport reader.

5.2 To this end, ICAO has developed a number of mandatory and optional security measures to protect the microchip from unauthorised access or manipulation. These measures aim to:

- protect the privacy of ePassport holders by preventing unauthorised access to their personal data (for example, through skimming⁶¹ and eavesdropping⁶²);
- validate that the ePassport presented at the border was issued by a bona fide authority; and
- confirm that the microchip is not a clone⁶³ and has not been altered after passport issuing.

⁶¹ Skimming involves accessing the data on the microchip through a covert ePassport reader without the authority or knowledge of the passport holder.

⁶² Eavesdropping occurs when a covert ePassport reader intercepts without authorisation a legitimate communication between an ePassport and an ePassport reader.

⁶³ A cloned microchip is a replica of an original and authentic passport microchip, including the original information. A cloned microchip could be inserted into a different ePassport for the purpose of committing imposter fraud (discussed in Chapter 4).

5.3 The APO has implemented the required ICAO security measures to meet these aims (outlined in Table 5.1).⁶⁴

Table 5.1

Electronic measures to enhance the security of the Australian ePassport

Measure	Purpose
Basic Access Control	Basic Access Control locks the microchip until the ePassport's machine readable zone is swiped. It seeks to prevent the data on the microchip from being skimmed or eavesdropped.
Passive Authentication	<p>Passive authentication seeks to provide assurance that the data on the microchip:</p> <ul style="list-style-type: none"> • was put there by the Australian Government; and • is complete and has not been changed since the passport was issued. <p>Passive authentication is implemented through the use of Public Key Infrastructure established by ICAO.</p>
Active Authentication	Active authentication seeks to provide assurance that the microchip contained in the ePassport is the original and not a clone.

Source: ANAO analysis of publicly available information.

5.4 The effectiveness of each of these security measures and other controls is discussed below.

Protecting the microchip from unauthorised access: Basic Access Control

5.5 Basic Access Control (BAC) links the physical control of the ePassport booklet with the ability to read its microchip. BAC is an encryption system that requires the ePassport's machine readable zone to be read to allow access to an electronic key that unlocks the microchip. The requirement to manually scan the machine readable zone prevents unauthorised and remote access to information on the microchip.

5.6 BAC has been included in each version of the Australian ePassport as the result of a recommendation made by the then Office of the Federal Privacy Commissioner (OFPC) in 2005 to reduce the threat of skimming and eavesdropping. Nevertheless, BAC has certain reported vulnerabilities, most notably that prior knowledge of an ePassport's machine readable zone and

⁶⁴ Chapter 2 discusses the international interoperability testing that confirmed the Australian ePassport's compliance with mandatory ICAO requirements. The key mandatory electronic security requirement is passive authentication.

'brute force' attacks could theoretically be used to defeat BAC encryption (see Figure 5.1).

Figure 5.1

Potential methods of defeating the BAC encryption system

<p>Prior knowledge of the machine readable zone</p> <p>A passport reader is used to unlock the BAC using prior, or partial, knowledge of data from the ePassport's machine readable zone.⁶⁵</p> <p>ANAO comment:</p> <ul style="list-style-type: none">• The machine readable zone contains most of the useful information that is accessible on the ePassport's microchip.⁶⁶ Therefore, prior knowledge of the machine readable zone would limit the value of also reading the microchip.
<p>Brute force attack</p> <p>A passport reader is used to check all possible electronic keys to identify the correct BAC key.</p> <p>ANAO comment:</p> <p>There are three significant limitations to a brute force attack:</p> <ul style="list-style-type: none">• to successfully defeat BAC encryption, the attacker requires partial prior knowledge of the ePassport's machine readable zone to reduce the number of possible electronic keys;• the covert passport reader needs to be close to the ePassport's microchip to generate enough power for it to start⁶⁷; and• the microchip needs to remain within range of the reader for a significant period of time to enable the encryption system to be defeated (even where the number of possible electronic keys has been significantly reduced). <p>Any covert attempt at skimming or eavesdropping is therefore likely to be obvious to the passport holder.</p>

Source: ANAO analysis of publicly available information.

5.7 The then OFPC and ICAO recommended BAC as the best option for reducing the threat of skimming and eavesdropping on the microchip. The APO's implementation of these recommendations in compliance with ICAO standards provides reasonable assurance that BAC is fit for purpose. In addition, any possible attempts to defeat BAC encryption would require technical knowledge and the assumption of risks (such as proximity to the

⁶⁵ Partial knowledge of some of the data from the machine readable zone would assist in unlocking the BAC by reducing the number of possible encryption key combinations.

⁶⁶ The information contained within both the machine readable zone and the microchip includes the holder's name, date of birth, nationality, gender, passport number and its date of expiry. The additional information contained on the microchip is the holder's image and eye coordinates.

⁶⁷ The ICAO standards for reading the ePassport's RFID microchip require that its radio frequency signal range be a maximum of 10cm and that the microchip operate within a specified power range. In order to read the ePassport microchip from any distance greater than 10cm, special equipment including large antennae would be required to mitigate any power loss over the greater distance. The nature of this special equipment would decrease the portability and covert nature of the reading device.

ePassport) that exceed the benefits in gaining access to the information. In short, there are easier and lower risk methods to access the information, such as through physical access to the ePassport's biographical data page.⁶⁸

Locking the microchip to prevent write access

5.8 Effective security procedures are required to prevent fraudsters stealing and personalising blank passports without authority. The APO advised that possession of booklets is tightly controlled and logged and that it locks the microchip with a security code. The microchip is only unlocked for writing during the personalisation stage, and is then re-locked to prevent further write access. In addition, the APO advised that control of the security codes is separated from control of the booklets, which limits the risk of internal fraud. However, the APO has not documented this process nor conducted vulnerability assessments (discussed in Chapter 6) to determine its adequacy in maintaining security. The ANAO suggests that there is merit in documenting these processes to enable future review.

Validating and verifying the microchip data: Passive Authentication

5.9 Passive authentication provides the capability to validate that a bona fide authority issued an ePassport and to verify that the data on its microchip remains unaltered since the passport was issued. This provides the border control authority with confidence that the ePassport is authentic.

5.10 Implementation of passive authentication involves the use of 'Public Key Infrastructure' (PKI), which uses two sets of public and private electronic keys for each ePassport. These are known as the Country Signing Certificate Authority (CSCA) keys and the Document Signing Certificate (DSC) keys. The APO creates the CSCA public and private key. The CSCA private key is then used to generate a pair of DSC public and private keys. The DSC private key is used to digitally sign the personal data stored on the ePassport microchip.

5.11 The CSCA and DSC public keys are exchanged with other countries through established protocols⁶⁹ and the DSC public key is also stored on the

⁶⁸ For example, see the Department of Foreign Affairs and Trade, *Annual Report 2010–11*, 5 October 2011, p.156, which notes that 36 161 passports were lost or stolen in that financial year.

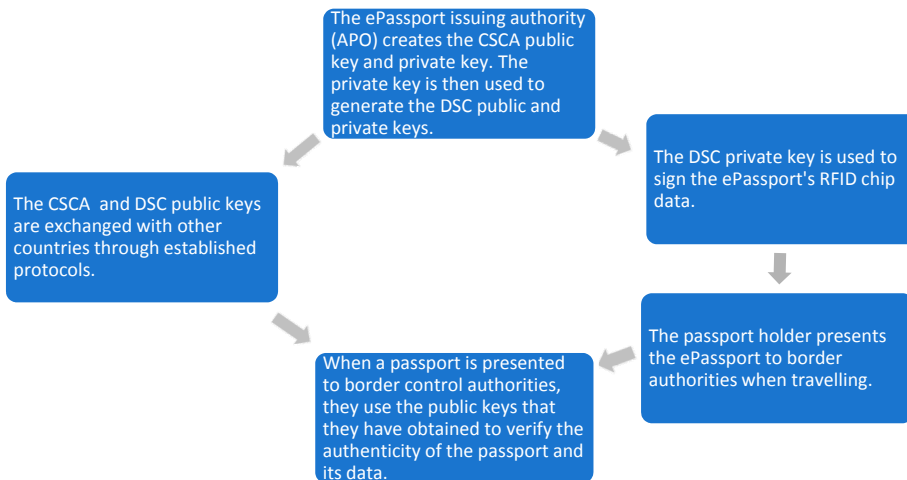
⁶⁹ The protocols involve the exchange of the CSCA public key through diplomatic means or via a CSCA Master List issued by the Public Key Directory, and the publishing of the DSC public key in the ICAO Public Key Directory that is accessible by all countries.

ePassport. Both of the private keys are secured in the APO's passport issuing system.

5.12 The CSCA and DSC public keys are both required by border control authorities to validate that the ePassport was issued by an appropriate issuing authority and to verify that the data on the microchip has not been changed. This process is illustrated in Figure 5.2.

Figure 5.2

The public key infrastructure process



Note: Should an ePassport issuing authority have a serious concern regarding the security of its certificates, it will issue a Certificate Revocation List. All Certificate Revocation Lists are loaded to the ICAO Public Key Directory for access by border authorities from all countries. The APO advised the ANAO that it used Certificate Revocation Lists to revoke certificates issued as part of its ePassport trials, but it has not used them since.

Source: ANAO analysis of publicly available information.

5.13 ICAO standards require complex cryptographic algorithms to be used for passive authentication. The integrity of these complex cryptographic algorithms is critical to provide assurance of the passive authentication process. The Information Security Manual produced by the Defence Signals Directorate notes with regard to these (and other similar algorithms) that:

There is no guarantee or proof of security of an algorithm against presently unknown attacks. However, the algorithms listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible attacks. There have been some cases where theoretically impressive

vulnerabilities have been found, however these results are not of practical application.⁷⁰

5.14 The APO has implemented cryptographic algorithms as required by ICAO and endorsed by the Information Security Manual. Therefore, cracking passive authentication cryptographic algorithms is not currently viable or practical given the computing power required. Even as technology develops, and assuming that the passive authentication cryptographic algorithms remain unchanged, defeating PKI security would require significant technical knowledge and resources. As such, PKI provides a reasonable assurance that the data contained on the Australian ePassport's microchip is authentic and remains unaltered since the passport was issued.

Protecting the microchip from cloning: Active Authentication

5.15 Active authentication aims to protect ePassports against microchip substitution with cloned or copied microchips. In accordance with ICAO standards, the implementation of active authentication involves the creation of a public and private key pair. However, unlike passive authentication, these keys are both stored on the microchip. The public key is accessible to border control passport readers while the private key is stored in the microchip's secure memory and cannot be accessed or copied from one microchip to another. Upon reading the public key, the passport reader challenges the microchip to respond using its private key. Given that the private key cannot be copied from one microchip to another, a correct response to the passport reader from the microchip provides assurance that the microchip is genuine.

5.16 The APO introduced the active authentication capability in 2009 as an additional security feature for the 'N' series ePassport. Therefore, 'M' series ePassports issued prior to 2009 do not have this capability and may be at greater risk of being cloned than the 'N' series ePassport. However, given that the use of cloned ePassports would be limited to imposters with a similar appearance to the original passport holder, the APO has assessed this risk as small.

5.17 Nevertheless, in recognising the operational imperative to introduce the active authentication capability, the ANAO suggests that, in addition to

⁷⁰ Defence Signals Directorate, *Australian Government Information Security Manual – Controls*, 2012 Canberra, p.182 <<http://www.dsd.gov.au/infosec/ism/index.htm>> [accessed 9 December 2011].

monitoring fraudulent ePassports for any evidence of cloning through its document examination capability (discussed in Chapter 4), the APO should also seek to brief other agencies on this issue in the context of its reinvigorated strategic intelligence capability (discussed in Chapter 2).

Controls to protect the ePassport's security architecture

5.18 To maintain the integrity of the ePassport's security architecture, it is important that security procedures and controls are appropriately documented. Appropriate documentation would:

- support APO staff to follow the correct security procedures, such as maintaining the segregation of duties, and assist new staff to learn their roles;
- facilitate future upgrades of the system; and
- facilitate monitoring and review of adherence to security controls and policies.

5.19 The ANAO requested documentation regarding the APO's ePassport security architecture but was advised that it relied primarily on ICAO documents as guidance. The ANAO notes that the ICAO documents provide detailed and complex guidance in relation to its standards, but they do not describe the APO's operational arrangements for implementing those standards.

5.20 While reliance on the ICAO documents is sound practice in the design of the security architecture, the lack of documentation to outline the APO's implementation makes review difficult and creates significant risks. In the context of ePassport security, the risk is that vulnerabilities in the system are more difficult to review and identify and the loss of key staff would create a knowledge gap. Developing and maintaining appropriate documentation would assist with the future review of systems and processes. As a result of these findings, the APO has undertaken to develop PKI documentation by June 2012.

Evidence of electronic security features being compromised

5.21 International media reports in recent years have variously suggested that ePassports are vulnerable to skimming, eavesdropping and cloning. The ANAO reviewed this reporting and sought to identify any instances where the

security of the Australian ePassport's microchip had been compromised. This involved:

- reviewing APO files and documents;
- reviewing international reporting, including ICAO material; and
- interviewing APO staff and discussing the issue with stakeholders, including the AFP, the Department of Immigration and Citizenship and the Defence Signals Directorate.

5.22 The ANAO noted that there are no known instances of fraudsters successfully overcoming the electronic security of the Australian ePassport to clone the microchip or alter the information on the microchip. The APO confirmed that there are no known instances of data on the microchip being altered. The ANAO noted in this regard that the APO monitors media reports and responds to them internally via briefs to the DFAT Senior Executive and Ministers as appropriate. In addition, the APO contributed to an ICAO paper that seeks to refute common claims about ePassport vulnerabilities.⁷¹

5.23 Notwithstanding the lack of evidence of the microchip's security features being overcome, it is likely that some individuals and organisations with technical knowledge and skills will seek to do so in the future, which reinforces the importance of ongoing monitoring in this area. In addition, while the ePassport's security features may be adequate if effectively implemented, practical or procedural weaknesses may only be revealed through independent vulnerability testing. This issue is discussed in Chapter 6.

Conclusion—Securing and verifying ePassport data

5.24 The ePassport employs a number of electronic security features that provide protection against a range of potential threats. These measures, combined with the booklet's security features, make the task of producing a fraudulent passport significantly more complex than it was prior to the introduction of ePassports. While media reports have suggested that ePassports are vulnerable, there are no known instances of fraudsters successfully overcoming the electronic security features of the Australian ePassport.

⁷¹ ICAO – *39 myths about e-passports*, Keesing Journal of Documents & Identity, Issue 30, 2009.

Managing privacy aspects of ePassports

5.25 The Australian passport is widely recognised as one of Australia's premier identity documents and, with around 48 per cent of the Australian population holding one, the APO controls significant amounts of personal data, including biometric information. It is therefore important that appropriate measures are employed to secure this information and protect holders' privacy in accordance with the *Privacy Act 1988* (Privacy Act). While the previous section examined the security of personal information contained on the ePassport's microchip, this section assesses the APO's:

- management of the ePassport's impact on privacy;
- approach to privacy training and awareness;
- arrangements for monitoring access to its databases; and
- privacy record.

Managing the impact of the ePassport on privacy

5.26 The introduction of the ePassport did not change the type of information collected from applicants. ICAO selected the face as the only mandatory biometric for the ePassport partly because photographs were already collected in the passport application process. Nevertheless, the use of FR technology to determine eligibility and verify the passport holder's identity at the border has expanded the use of passport photographs and reinforces the importance of effectively managing and protecting personal data.

5.27 To assess the impact of the ePassport on privacy, the APO conducted a Privacy Impact Assessment in 2004.⁷² In addition, the APO consulted with the then OFPC at an early stage with the OFPC receiving Government funding to conduct privacy audits of the ePassport in 2005 and 2006.⁷³ A key finding of

⁷² The Office of the Australian Information Commissioner (formerly the OFPC and the Office of the Privacy Commissioner) suggests that agencies undertake privacy impact assessments in managing projects involving personal information.

⁷³ Office of the Federal Privacy Commissioner, *ePassport & SmartGate Trial – Department of Foreign Affairs and Trade and Australian Customs Service*, October 2005 and Office of the Privacy Commissioner, *ePassports – Department of Foreign Affairs and Trade*, June 2006.

those audits was that the ePassport complied with the requirements of the Privacy Act.⁷⁴

5.28 Given the potentially sensitive nature of ePassports and the collection of biometric information, the development of a Privacy Impact Assessment and the APO's early engagement with the OFPC was sound practice. There would be merit in the APO taking a similarly robust approach to managing privacy for any future passport development projects that have additional privacy impacts.

Training, guidance and privacy awareness

5.29 The then OFPC also found in its privacy audits that the APO had a strong culture of privacy protection. Maintaining that culture requires ongoing training, guidance and practices that promote awareness of the need to protect privacy.

5.30 The APO advised the ANAO that its staff are aware of their privacy obligations and that privacy is a large focus of its day-to-day business. In reviewing relevant documentation and interviewing staff, the ANAO confirmed that APO operations have an adequate focus on protecting privacy. For example, the APO:

- provides a number of training courses that cover privacy aspects;
- provides a privacy warning to staff when logging onto passport processing and issuing systems; and
- is proactive in managing privacy in meetings and through Memoranda of Understanding with other agencies.

5.31 The APO Canberra also conducts a structured induction program that includes a mandatory requirement for new staff to complete a self-paced online privacy module.⁷⁵ In addition, staff can access the module to undertake refresher training at any stage. However, at the time of the audit, refresher

⁷⁴ In the 2005–06 Budget, the OFPC received \$0.7 million over four years to provide privacy and audit advice in relation to the *Providing for Australia's Security – Biometrics for Border Control* program.

⁷⁵ The APO Canberra is currently reviewing its induction program and plans to implement a revised version across all APO offices to encourage consistency. The APO has about 35 online Passport Electronic Training modules that staff can access at any time. Passport Electronic Training module 02 is entitled *Privacy and FOI principles*.

training on the module was not mandatory, nor was a record kept of those who undertook it.

5.32 The ANAO considers that the APO's current approach to maintaining a culture of privacy awareness is adequate. Nevertheless, there would be merit in requiring staff to undertake refresher training periodically (e.g., biennially) to ensure they maintain their knowledge and keep up-to-date with developments. Monitoring the completion of such refresher training would help to provide management with assurance in this regard. In response, the APO advised that it has now put in place a system to track completion of relevant training and to highlight those due for refresher training.

Monitoring access to passport databases

5.33 Systematically monitoring staff access to the APO's personal data holdings is important to help prevent inappropriate access to, and the misuse of, this information. Monitoring should include strategies to reasonably assure the APO that individuals are not breaching their privacy obligations.

Passport Issue and Control System

5.34 The APO stores and maintains the personal data submitted by passport applicants in its Passport Issue and Control System (PICS). The APO advised the ANAO that staff have access to PICS only when relevant to their role and that a list of all those with access is maintained. In addition, some DIAC staff have limited access to PICS to assist them with their border control functions.⁷⁶ Staff from other agencies, including the AFP, do not have direct access to PICS and must request information in writing.

5.35 While all access to the PICS database is logged in an electronic audit trail, the APO does not proactively use this facility to identify potentially inappropriate access. For example, the APO does not cross-reference the applications that an Eligibility Officer has processed with the PICS records that they have accessed unless a specific issue arises. In addition, the APO has limited indicators or alerts to identify inappropriate access to the PICS database. This creates the risk that APO staff could access the personal records of passport holders without detection.

⁷⁶ The APO advised that DIAC staff may only access PICS records by inserting known passport numbers, which prevents browsing.

5.36 In response to these concerns, the APO noted that audits of staff access to personal data would be difficult to undertake and may be of limited value. The ANAO acknowledges these concerns, but notes that other government agencies with significant personal data holdings have established control frameworks to help detect browsing and inappropriate access by staff.⁷⁷ It also notes that the Australian Public Service Commission's *State of the Service Report 2010–11* identified, through an agency survey, 145 instances of improper access to personal information (e.g., browsing) across the public service.⁷⁸

5.37 To increase management assurance that access to personal data is appropriate, there would be benefit in the APO developing a control framework to help address this risk. For example, randomly auditing the PICS access of five officers each month would provide coverage of 60 officers a year, equating to about 12 per cent of the 500 officers with access. A first step would be to consult with other agencies with similarly large holdings of personal information to identify suitable monitoring approaches.

Checking access to personal records considered to be at high risk

5.38 The APO maintains a list of passport holders whose personal information is considered to be at increased risk of inappropriate access by staff. Each month, the APO identifies those staff who have accessed the records of individuals on the list and assesses whether that access was appropriate. If access is considered to have been inappropriate, the APO Senior Executive receives a written report and the staff member may be referred to DFAT's Conduct and Ethics Unit for further investigation.⁷⁹

5.39 At the time of the audit, there were 109 passport holders on the list. However, there was no guidance on when an individual should be added or removed from the list, and no facility to record the reasons why such action was taken.

⁷⁷ For example, see *Centrelink Fraud Control Plan 2008–10*, July 2009, p.55, <http://www.humanservices.gov.au/spw/corporate/freedom-of-information/resources/disclosure-log/centrelink_fraud_control_plan_2008-10_v2.pdf> [accessed 22 February 2012], which states that a control framework for the prevention, detection and deterrence of browsing and inappropriate access to customer information is in place in Centrelink.

⁷⁸ Australian Public Service Commission, *State of the Service Report 2010–11*, p.71

⁷⁹ The APO advised that three staff of a third party contractor had been identified as having accessed passport holders' records inappropriately in 2010–11. The APO also advised that these incidents had been referred to the management of the third party contractor who had taken appropriate action.

5.40 Overall, the approach is a useful method of monitoring staff access to those passport holders considered to be at increased risk of inappropriate access. However, the absence of guidance on the operation and maintenance of the list increases the risk that its coverage is inappropriate or out of date. Therefore, there would be merit in the APO documenting the arrangement and clearly defining the criteria used for adding and removing passport holders.

Facial images stored in the FR database

5.41 The APO maintains a separate database which holds applicants' images once the passport has been issued. The APO advised that the FR system operates in the background of the application process and that staff cannot access the images outside the context of the application they are currently processing. Therefore, the APO considers that monitoring access to the FR database is not required. However, the system administrators have access to enable information to be changed if required. The ANAO suggests that, to provide appropriate safeguards for information in the FR database, there would be merit in the APO conducting periodic checks of the FR database logs to assure itself that any changes are appropriate.

The APO's privacy record

5.42 The Office of the Australian Information Commissioner (formerly the OFPC) is responsible for receiving and investigating complaints about possible breaches of privacy by federal government departments. The Office of the Australian Information Commissioner advised the ANAO that it has not received a complaint about the APO since ePassports were introduced in 2005. This would suggest that the APO has a sound record in managing and protecting privacy.

Conclusion—Managing privacy aspects

5.43 The APO put in place effective arrangements to manage the privacy of individual passport holders following the introduction of ePassports in 2005. While the APO's current approach to maintaining a culture of privacy is adequate, there would be merit in requiring staff to undertake periodic refresher training and monitoring that training. In response, the APO advised that it has now put in place a system to track completion of training and to highlight those due for refresher training.

5.44 While access to the PICS database is logged in an electronic audit trail, the APO does not proactively use this facility to identify potentially inappropriate database access. A small number of periodic random audits

would increase management assurance that access to personal records is appropriate. The APO monitors staff access to a limited number of high-risk records, however, the arrangement and criteria used for adding and removing passport holders to this list have not been documented.

6. Monitoring ePassport Vulnerabilities and Client Satisfaction

This chapter assesses the adequacy of the APO's approach to monitoring ePassport vulnerabilities and managing risk. It also examines whether the APO has an appropriate focus on client satisfaction, and effectively monitors its performance in relation to the ePassport.

Vulnerability testing and risk management

6.1 As technology advances and becomes cheaper to acquire, fraudsters may increasingly seek to defeat the security features of the ePassport. Maintaining the security of the ePassport requires processes to identify, monitor and manage emerging vulnerabilities and risks. Without adequate management of these issues, confidence in the Australian passport as a high-quality identity document may be reduced. This is particularly important in light of the 10-year life of the Australian ePassport.

6.2 The ANAO assessed the APO's approach to ePassport vulnerability testing and risk management by reviewing its arrangements for:

- maintaining an adequate supply of passport booklets;
- testing the microchip for robustness;
- testing the ePassport booklet and its electronic security features for vulnerabilities; and
- managing fraud risks and general risks.

Maintaining an adequate supply of ePassport booklets

6.3 The production of blank passport booklets that meet both international standards and Australian requirements involves a complex process that cannot be quickly transferred to another supplier should a problem occur in the production process. This means that risks to the ongoing production and supply of booklets need to be effectively managed, with contingency plans put in place to cover potential disruptions.

6.4 The long-standing approach to managing this issue involves the stockpiling of an adequate supply of blank booklets.⁸⁰ However, following the depletion of stock to critically low levels, the APO implemented a strategy in 2009 to stockpile one year's supply of booklets as a contingency buffer against interruptions to production. While this provides an adequate approach to managing supply continuity risks⁸¹, the ANAO suggested that, to help avoid a recurrence of stock depletion, its approach to managing supply be included in an APO-wide risk register to facilitate regular monitoring and review. The APO advised that it has now done this.

Testing the microchip for robustness

6.5 The insertion of microchips into passport booklets introduced the potential for microchip failure and inconvenience to the passport holder. The failure of a significant number of microchips could damage the APO's and Australia's reputation for issuing high-quality identity documents. Therefore, it is important that the microchip be sufficiently robust to survive the rigours of passport production and ordinary passport use for its 10-year life.

6.6 The ANAO's file reviews revealed that the APO has adopted a sound approach to managing the risk of microchip failure. In particular:

- the APO obtained a 12-year microchip warranty, which is sufficient for the 10-year life of the passport and a two-year contingency buffer;
- the APO, Note Printing Australia (NPA) and the microchip manufacturer tested the robustness of the microchip during the development of the first 'M' series ePassport and found that it would withstand reasonably harsh treatment⁸²;
- the microchip was tested in international interoperability trials prior to the introduction of ePassports in 2005 (discussed in Chapter 2); and
- NPA tests the functionality of each microchip as it is inserted into the booklet.

⁸⁰ ANAO Audit Report No.37 2002–03, *Passport Services*, noted that the risks to continuity of supply of passport blanks had been addressed through the stockpiling of blanks (p.24).

⁸¹ Note Printing Australia, the passport booklet manufacturer, advised the ANAO at the time of the audit that passport booklet stock exceeded the 12 months requirement.

⁸² ICAO has established a standard for testing the durability of ePassports (*Machine Readable Travel Documents: Technical Report – Durability of Machine Readable Passports v3.2*, ICAO, 30 August 2006).

6.7 The APO advised that only one microchip has failed due to an inherent fault since the ePassport was introduced.⁸³ This is particularly noteworthy given that some 8.8 million Australian ePassports have now been issued (as at 31 January 2012) since 2005.

Storage capacity of the microchip

6.8 ICAO requires microchips to have a minimum storage capacity of 32 kilobytes but does not specify a maximum capacity. The APO selected a 512 kilobyte microchip for the Australian ePassport which was substantially larger than that used in most ePassports introduced at that time.⁸⁴ The APO advised that the microchip was selected to provide flexibility to manage potential changes in international standards⁸⁵, and that there were only marginal additional costs associated with the larger microchip.

6.9 In light of the fact that Australia was one of the first countries to introduce an ePassport, the ANAO concluded that the selection of the large microchip was probably prudent at the time. The APO is now considering reducing the size of the microchip to be used in the next passport series (the 'P' series) to 256 kilobytes. This appears to be a sensible approach.

Inclusion of secondary biometric identifiers on the microchip

6.10 As noted in Chapter 2, the facial image is the primary biometric identifier specified by ICAO, with secondary biometrics such as fingerprints or iris optional.⁸⁶ While the Australian ePassport uses only the face, many other ePassport issuing countries store fingerprints as a secondary biometric in their ePassports or have plans to do so in the future.⁸⁷

⁸³ Microchips have failed after the passport has been issued due to accidental or deliberate damage. For example, where the holder has attempted to dry the booklet in a microwave, or a poorly directed immigration stamp has damaged the microchip.

⁸⁴ Most countries that introduced ePassports during 2005 or 2006 chose a 64 or 72 kilobyte microchip. However, the ICAO New Technology Working Group concluded in its technical report '*Biometrics Deployment of Machine Readable Travel Documents*' (21 May 2004, pp.36-37) that countries should target towards using a microchip of 512 kilobytes or more to facilitate future-proofing.

⁸⁵ While the photograph stored on the microchip requires only about 20 kilobytes, the APO would not need to change microchips if a second biometric (discussed in this chapter), such as fingerprints, became an international requirement.

⁸⁶ ICAO, *Machine Readable Travel Documents Part 1 Volume 2*, 2006, 6th edition, ICAO (p.I-1).

⁸⁷ As at July 2011, 45 of the 93 ePassport issuing states included both face and fingerprints and a further 14 states had plans to do so. For example, the European Union requires the inclusion of the fingerprint as a secondary biometric for its members' passports. APO advised that countries collecting fingerprints use this information internally rather than for border security purposes.

6.11 The APO advised that it maintains a general interest in the use of secondary biometrics and recognises their potential to enhance passport security. The APO has not assessed the costs and benefits of implementing a secondary biometric but believes that it would be complex and expensive to do so. In addition, the APO considers that there is no security imperative or appetite in the Australian community to include secondary biometrics at this stage. Any future consideration of the use of a secondary biometric for the Australian ePassport would ultimately be a policy decision for the Government.

Vulnerability testing of the passport booklet

6.12 While the introduction of the ePassport added an additional electronic security layer to the Australian passport, the physical security features of the booklet itself remain a central pillar of passport security. Assurance that these features remain effective requires ongoing vulnerability testing of the passport booklet, including the paper, inks, adhesives and laminates, and the arrangements for the physical incorporation of the microchip into the booklet.

6.13 To this end, the APO contracts NPA to design, develop, test and manufacture its passport booklets. Testing takes place both prior to the introduction of a new passport series and on an ongoing basis during production.⁸⁸ In addition to this testing, the APO also provides samples of booklets to a number of government agencies for vulnerability testing.⁸⁹

6.14 The ANAO reviewed the APO's testing approach for the 'N' series passport booklet and concluded that the approach was sound. In particular, testing of the centre page containing the microchip indicated that attempts to remove it resulted in obvious damage to the booklet.

Vulnerability testing of the microchip's security features

6.15 As noted in Chapter 5, while the ePassport's various security features such as BAC and PKI are generally sound, they need to be effectively applied to optimise their efficacy. In addition, technological advances may see new

⁸⁸ For example, NPA conducts quality assurance testing of the booklets by testing two consecutive booklets for every 16 000 it produces.

⁸⁹ For example, with the current 'N' series booklet, samples were provided to the AFP, DIAC and the Commonwealth Scientific and Industrial Research Organisation to enable various aspects of the 'N' series booklet to be tested.

threats to the ePassport emerge over time. Reflecting these risks, the DSD's Information Security Manual recommends that agencies undertake independent vulnerability assessments prior to the introduction of new systems and also annually to monitor the threat environment.⁹⁰

6.16 The APO intended to engage a contractor to undertake vulnerability testing of the microchip in 2008, but this did not eventuate.⁹¹ In addition, around that time an internal minute to the APO Senior Executive recognised the importance of external vulnerability testing and recommended that an external e-Security expert such as DSD be engaged to conduct a series of audits to ensure that the ePassport complies with security requirements. However, a vulnerability assessment of the application of the ePassport's security features was not conducted at that time.

6.17 The issue of ePassport security has also been raised by the Australian Parliament from time to time. For example, in 2008 the Parliamentary Joint Committee on Intelligence and Security requested information from DSD about the vulnerability of ePassports (see Figure 6.1).

Figure 6.1

Parliamentary Joint Committee on Intelligence and Security—Question on Notice (28 August 2008)

Question: There was a report in the media recently that some whiz kids had been able to break the e-passport standard and manufacture false passports. Is that an issue that would find its way to DSD for your prowess in the security end of it?

Response:

- a) DFAT has not requested DSD's assistance in relation to the claims that vulnerabilities exist in e-passports.
- b) This is an issue that DSD could be asked to provide advice on. As the national authority for information security, DSD provides advice to Australian federal and state authorities to protect information and communication technology products and networks.

Source: Letter of 1 July 2009 from the Defence Signals Directorate to DFAT.

6.18 The Parliamentary Joint Committee on Intelligence and Security also sought DSD's advice in 2009 on the ePassport's security for its inquiry into the administration and expenditure of Australian intelligence agencies. The

⁹⁰ Defence Signals Directorate, *Australian Government Information Security Manual*, Canberra, (pp.58-60).

⁹¹ The APO advised that this testing did not proceed due to problems encountered by the contractor in obtaining a suitable microchip reader.

Committee noted international reporting had suggested that ePassports of other countries had been 'cracked'. This raised the Committee's concern that the Australian ePassport may also be vulnerable. In conclusion, the Committee reported that it:

sought advice from DSD about potential vulnerability of Australia's e-passports. DSD provided a classified response that satisfied the Committee on this matter.⁹²

6.19 Notwithstanding the Committee's interest, the APO had not pursued independent vulnerability testing of the Australian ePassport's security features at the time of this audit. Instead, the APO advised that it was satisfied with ICAO's work in the development of ePassport security standards and features and that these features had been conceptually proven as effective.⁹³ In addition, the microchip is only one element of the overall security package of the passport booklet.

6.20 The ANAO discussed the issue of ePassport microchip vulnerability testing with DSD. DSD advised that the ePassport should be moderately secure, provided its electronic security features are applied effectively. DSD considered it important for independent vulnerability testing of the Australian ePassport's security features to be undertaken and advised that this work could be performed by DSD, depending on the availability of resources, or by another suitably qualified organisation.

6.21 In response to these findings, the APO advised that it has now engaged DSD to carry out a vulnerability assessment. While the terms of reference of the vulnerability assessment had not been finalised at the time of the audit, the APO anticipates that the work will be completed by mid-2012. The need for further vulnerability testing should be reviewed periodically in consultation with DSD to identify emerging threats and so that further independent vulnerability testing may be conducted as required.

⁹² Parliamentary Joint Committee on Intelligence and Security, *Review of Administration and Expenditure No.7 – Australian Intelligence Agencies*, May 2010 (pp.29-30).

⁹³ The APO advised the ANAO that ICAO and other appropriate standards bodies investigate and report on all claims regarding the vulnerability of ePassport's electronic security features and that in all cases the claims have been found to be false or without proof of substance.

Managing fraud risks

6.22 The APO identifies and manages passport fraud risks through input to regular DFAT-wide Fraud Control Plans. The key passport risks and treatments identified in the Fraud Control Plan 2011 are listed in Table 6.1.

Table 6.1

Key passport fraud risks and treatments

Key risks	Examples of the risk treatments identified
<ul style="list-style-type: none"> • Altering of genuine passports • Issue of fraudulent or duplicate passports • Illegal use of passports by impostors • False information and documents in support of applications 	<ul style="list-style-type: none"> – Research into, and development of, document construction and processes that maintain integrity, including implementing improvements in facial recognition technology. – Participation in whole-of-government initiatives, forums and activities as they relate to identity crime and cooperation with border control agencies at strategic and operational levels. – Increase validation of presenting identification documents—implement improvements in technical processes and data cross checking. – Create an intelligence area within Passport Fraud Section for data matching purposes and adopt data analytic techniques to enhance fraud prevention and detection.

Source: Department of Foreign Affairs and Trade, *Fraud Control Plan 2011*, DFAT (pp.16-17 and 68-74).

6.23 Overall, the Fraud Control Plan adequately covers the key passport fraud risks and treatments.

Managing general passport risks

6.24 The effective management of passport risks is important because the APO operates in a fluid international security environment and operates specialised and complex systems that provide secure identity documents to millions of Australians. At the time of the ANAO's audit, the APO relied on two formal processes to identify risks:

- at the strategic level, it listed seven risks in DFAT's agency-wide Risk Register 2011–12 and one risk in the DFAT Critical Risk List 2011–12. These risks include the issuing of fraudulently obtained genuine passports, the loss of key staff and the failure to deliver the Passport Redevelopment Program; and
- at the project level, it prepared risk management plans for specific projects.

6.25 The APO also monitored risks through its participation in domestic and international stakeholder meetings.

6.26 Notwithstanding these approaches, at the time of the audit the APO did not have an up-to-date formal risk management plan covering its key strategic and operational risks, which would impede their regular and systematic review.⁹⁴ In response, the APO advised that it has now developed a risk management strategy to actively manage its risks, and to facilitate the identification, monitoring and review of those risks at both the strategic and operational levels. This includes a detailed APO risk register with controls and treatments which, it advised, will be reviewed at monthly APO meetings and used to support quarterly reporting to the DFAT Senior Executive.

Conclusion—Vulnerability testing and risk management

6.27 The APO has adopted a sound approach to managing the risk of microchip failure, including robustness testing of the microchip during the development of the first ePassport and obtaining a 12-year warranty on the microchip from the manufacturer, and had found only one microchip that had failed due to an inherent fault.

6.28 The APO has also adopted a sound approach to testing the physical security features of the booklet, but relies on internationally proven electronic security features to protect the microchip. While DSD has advised the ANAO that the microchip's electronic security features should be moderately secure provided they have been applied effectively, at the time of the audit the APO had not conducted independent vulnerability testing of their application. In response to these findings, the APO advised that it has now engaged DSD to carry out this testing. The need for further vulnerability testing should be reviewed periodically in consultation with DSD to identify emerging threats and so that further independent vulnerability testing may be conducted as required.

6.29 The APO has included key passport fraud risks in the DFAT-wide Fraud Control Plan, and seven strategic risks in the agency-wide Risk Register 2011–12. However, at the time of the audit, the APO did not have an up-to-date formal risk management plan covering its key strategic and operational risks, which would impede their regular and systematic review. In response, the APO advised that it has now developed a risk strategy to actively manage its strategic and operational risks.

⁹⁴ The most recent APO Risk Management Register identified by the ANAO was dated 19 July 2004.

Recommendation No. 2

6.30 To strengthen the management of the ePassport's electronic security features, the ANAO recommends that the APO periodically review, in consultation with the Defence Signals Directorate, the need for further vulnerability testing of the application of these measures and, if required, arrange appropriate independent testing.

DFAT response

6.31 DFAT agrees with this recommendation. DFAT welcomes the ongoing involvement of the Defence Signals Directorate (DSD) in our ePassport program. We have commenced work with DSD on a vulnerability assessment project that will examine APO's implementation and integration of the Public Key Infrastructure (PKI). DSD has indicated a willingness to work with APO on future ePassport matters.

Monitoring client satisfaction and APO performance

6.32 It is recognised good practice to monitor client satisfaction because it allows the service provider to discover weaknesses and identify strategies to continually improve its services. In addition, performance monitoring and reporting reassures stakeholders that services are provided effectively and in accordance with policy. Ideally, performance monitoring should include measurable quantitative and qualitative indicators.

The APO's Client Service Charter

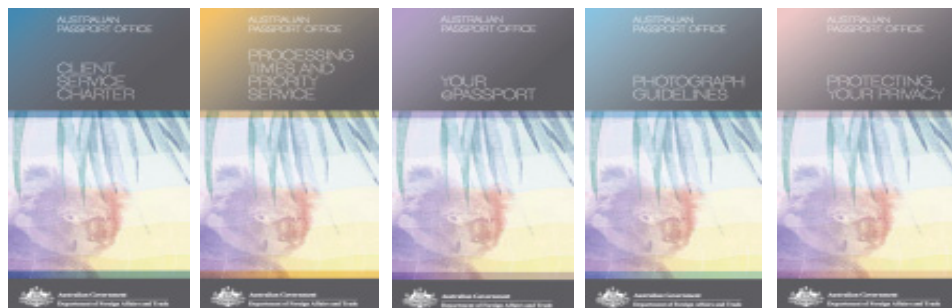
6.33 The APO's Client Service Charter advises clients that the APO aims to provide a secure, efficient and responsive passport service. The Charter outlines service standards that the APO seeks to achieve to satisfy its aim.⁹⁵ While the Client Service Charter does not specifically address the use of biometrics or the ePassport, the APO has developed a series of supplementary brochures that provide information to clients (see Figure 6.2 for some examples) on their rights and responsibilities.⁹⁶ Overall, the Charter and supplementary brochures help support an appropriate client focus.

⁹⁵ Service standards include displaying instructions about passport fees; being consistent in the way policy is applied; protecting information in accordance with privacy requirements; and providing a prompt service with clear and accurate information.

⁹⁶ Brochures can be readily accessed online or at passport offices.

Figure 6.2

Examples of APO brochures to support client service



Source: APO's website <<https://www.passports.gov.au/Web/index.aspx>> [accessed 17 November 2011].

Collecting and assessing client feedback

6.34 The APO advised that clients can provide feedback to it in a number of ways. For example, the Australian Passport Information Service (APIS) collects feedback received through its telephone and email information service.⁹⁷ While the reports on this feedback focus on quantitative criteria, they also provide some qualitative information on the nature of the feedback received.

6.35 Although the APO does not generally receive feedback specifically on ePassports and biometrics, it does receive complaints about passport photographs being rejected due to poor quality (the issue of photograph quality is discussed in Chapter 3).

6.36 In addition, clients may provide feedback directly to the APO on the service they receive from each state passport office. However, the two state offices visited by the ANAO reported that the feedback they receive is not routinely collected centrally, and one office advised that it generally discards anonymous feedback. At the time of the audit, the APO advised that it was developing a client feedback framework and that this will, in future, enable it to collect and analyse client feedback centrally. The APO also advised that it has developed a new feedback policy to enable a systematic approach to receiving, recording and analysing client feedback.

⁹⁷ The Australian Passport Information Service is a telephone information service available to callers within Australia. The service is available seven days a week and provides basic advice on such issues as applying for an Australian passport, documentation, lost and stolen passports, and application fees.

6.37 The APO also tests the quality of its services by conducting an annual 'Mystery Shopper' Program. This program involves an independent contractor using 'mystery shoppers' to pose as genuine users of passport services.⁹⁸ Each shopper assesses the service received against pre-defined criteria that are based on the APO's client service standards. The ANAO reviewed the Mystery Shopper Executive Report 2010 and noted that the percentage of clients satisfied with each of the APO's services had improved, from around the mid-80s to the low 90s, since 2008. The report did not identify any service issues relating to the ePassport.

6.38 The feedback received by the APO is generally positive. In addition, the APO advised that a recent benchmarking exercise undertaken with four other nations indicated that its client service performance was in advance of those countries.

Passport spoils and x-spoils

6.39 One of the APO's key performance indicators is monitoring and managing passport booklets 'spoiled' during the personalisation process and destroyed. 'X-spoils' occur post-issue and are the result of a failure of quality assurance during production and may cause substantial inconvenience to the passport holder. As passports are issued on a cost-recovered basis, spoiled and x-spoiled documents increase production costs and therefore unit costs.

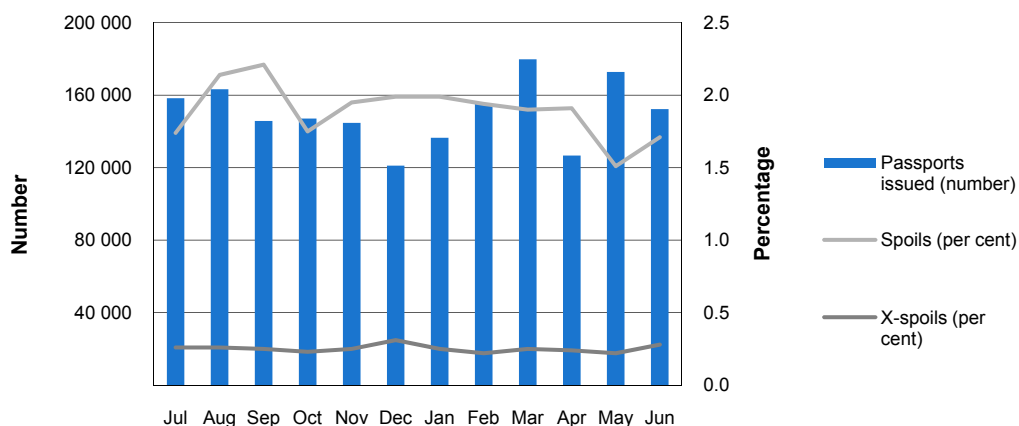
6.40 The APO's performance targets are 2 per cent for spoils and 0.3 per cent for x-spoils. In 2010–11, spoils totalled 36 745 and x-spoils 4 899 (Figure 6.3 shows spoils and x-spoils as a percentage of passports issued each month), with only 1 499 spoils (4.1 per cent of total spoils) and 56 x-spoils (1.1 per cent of total x-spoils) involving the microchip. The APO advised that these microchip-related spoils and x-spoils resulted from errors in the manufacture and personalisation of the passport booklets—for example, errors in writing data to the microchip⁹⁹—rather than faults with the microchip itself or with its security features.

⁹⁸ The services are randomly selected and include APO state and territory offices, some Australia Post outlets, APIS and the Consular Emergency Centre.

⁹⁹ For example, APO production staff may remove the booklet from the microchip writer before writing has been completed.

Figure 6.3

Monthly percentage of passports spoiled and x-spoiled 2010–11



Source: ANAO analysis of APO data.

6.41 In 2010–11 the APO consistently met its target for x-spoils and achieved its spoil target in 10 out of 12 months.

6.42 The APO advised that some microchip-related x-spoils occur when passport holders are referred to the APO by Customs and Border Protection because their ePassport is found not to be working at SmartGate. When the holder returns the passport to the APO the microchip’s functionality is checked with a passport reader and the APO invariably finds it to be functioning.¹⁰⁰ While APO’s policy is to replace these passports on the second occasion that a client complains, the ANAO’s visit to two state passport offices found that the policy is applied inconsistently.¹⁰¹ To encourage a consistent approach, there would be value in the APO reviewing and reissuing guidance on this matter.

Publicly available microchip readers at APO offices

6.43 The APO advised that it has installed ePassport microchip readers in the public areas of all passport offices across Australia, and at its offshore

¹⁰⁰ The APO advised the ANAO that the microchip always works and that the issue is more likely to relate to errors in using the SmartGate ePassport reader. Customs and Border Protection advised that it is currently implementing ePassport readers at all manual processing points at the main international airports. These readers will enable a manual check for those ePassports that could not be read at SmartGate. As a result, Customs and Border Protection considers that only ePassports with a genuinely faulty microchip will be referred to the APO in future.

¹⁰¹ While one office routinely replaced the passport, the other would only do so if a fault was found. Instead, it provided the holder with a letter confirming that the ePassport is operational.

production centres in London and Washington. These readers are intended to provide an opportunity for passport holders to independently check the data contained on the microchip.

6.44 Both of the passport offices visited by the ANAO had microchip readers that the public could use, although neither were signposted to identify their purpose or instruct clients in their use, and one kept the reader behind the counter (not publicly accessible) because it regularly malfunctioned or had been damaged by misuse. In addition, the availability of the readers is not advertised in any of the brochures available to clients or included on the passport application form.

6.45 To assist clients in accessing their personal information, and to promote the reliability of the microchip technology, there would be merit in the APO:

- ensuring that passport readers are publicly accessible in each of its offices, along with easy to follow instructions; and
- advising clients about the availability of the passport readers through its ePassport and/or privacy brochures.

6.46 The APO advised in this regard that it is in the process of replacing its passport readers with more robust and reliable readers. In addition, the APO is considering improving the signage in client service areas in relation to their use.

Key performance indicators and monitoring

6.47 Performance information should provide staff with timely feedback on program performance and assist managers and stakeholders to draw well-informed conclusions on performance.

6.48 The APO's objective is to provide Australians with access to secure international travel documents through the delivery of high-quality passport services. The APO uses two indicators to measure its performance against this objective (see Table 6.2).

Table 6.2

APO's 2010–11 Key Performance Indicators (KPIs)

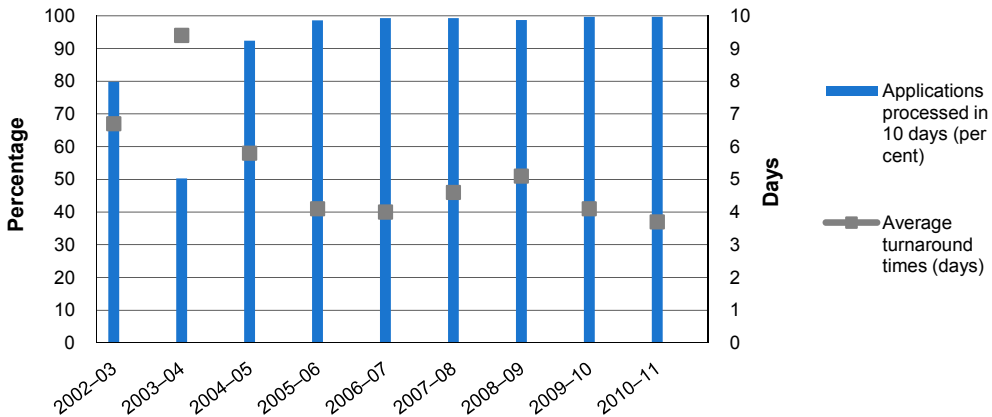
Key performance indicators	Stated achievements
Public and travel industry clients are satisfied with the department's efficiency and effectiveness in delivering passport services, with routine passports issued within ten working days and urgent passport issues dealt with in a timely and responsive manner.	<ul style="list-style-type: none"> • 99.7 per cent of applications processed within 10 working days. • Average turnaround time of 3.7 days. • Provided emergency passports for Australians involved in assisting with natural disasters in New Zealand and Japan. • Key player in the National Identity Security Strategy. • Commenced development of a new formal feedback policy. • Responded to 61 complaints through internal review and the Commonwealth Ombudsman.
The demand for passport services is managed effectively, including in a way that maintains security, efficiency and responsiveness, and that builds on information technology capabilities and innovative solutions.	<ul style="list-style-type: none"> • Demand for passport services increased by 1.65 per cent. • Increased resources for fraud investigation. • Worked on design of P-series passport. • 31 per cent of passports issued used online application forms. • Investigated 838 new cases of passport fraud.

Source: Department of Foreign Affairs and Trade, *Annual Report 2010–11*, October 2011 (pp.152-158) and APO advice.

6.49 The APO's main KPI is its target of issuing passports within 10 working days. The ANAO reviewed achievements against this indicator over the last nine years and found that the APO had been able to maintain this target notwithstanding the introduction of the ePassport in 2005–06 (see Figure 6.4).

Figure 6.4

KPI—10-day target for issuing passports



Source: APO statistics and DFAT Annual Reports.

6.50 The second KPI is more subjective than the first, making it more difficult to objectively compare one year's performance against another. While performance monitoring should be balanced with the cost of collecting, analysing and reporting information, there would be merit in the APO considering the development of a broader range of indicators to help evaluate its performance. The ANAO identified a number of potential indicators that may be useful in assessing passport integrity and performance, including:

- the percentage of new passport fraud cases identified prior to passport issuing;
- production spoilage; and
- feedback from clients.

6.51 In response, the APO has agreed to establish a broader range of quantitative and qualitative indicators.

Internal monitoring and reporting

6.52 An APO Business Assurance Unit was established in 2006 to undertake compliance checks and assist with identifying strategic business improvements. The Unit performs a useful quality assurance role for APO management. The Unit's role does not include reviewing the performance of the APO's FR system but, as described in Table 6.3, it does conduct monthly checks of certain FR functions.

Table 6.3**Business Assurance Unit's monthly facial recognition checks**

Checks	Process	ANAO Comment
High FR score not-merged	The records created when a passport holder is seeking to renew their passport should be merged with previous records of past applications. This monthly check involves re-assessing FR matching scores above 99.5 per cent where those records have not been merged.	Process contributes to the data integrity of APO databases. Missed cases of potential passport fraud may be identified.
Low FR score merged	This monthly check involves re-assessing passport applicants that have been merged with existing records and the FR matching score is less than 62 per cent. This may indicate that the two records are not the same person and have been incorrectly merged.	Process contributes to the integrity of APO databases.

Source: ANAO representation of APO data.

6.53 At the time of the audit, there was no policy documentation supporting these processes or the rationale for setting the thresholds at 99.5 per cent and 62 per cent. The APO advised the ANAO that the thresholds were set at:

- 99.5 per cent because any match that high would undoubtedly be the same person; and
- 62 per cent because any match that low would not be the same person.

6.54 Given that only one merging error was found out of 239 records checked in April 2011, there would be merit in the APO reassessing its thresholds and their rationale, and documenting the process. The APO advised that these issues will be addressed by June 2012 as part of its Future Directions Plan.

6.55 In addition to Business Assurance Unit checks, monthly and quarterly reports are prepared for the APO Senior Executive on the APO's performance against processing benchmarks and indicators, including: staffing levels, passport demand, spoilage rates, passport issuing times and fraud statistics. A quarterly report is also prepared for the DFAT Senior Executive.

6.56 The ANAO reviewed recent reports and found that they provide a useful overview of workload and performance over the reporting period in question. There are, however, opportunities to improve the reports by including a performance indicator on the FR system (such as the number of new fraud cases identified through that system), and by including graphs to compare current performance against longer-term trends.

Conclusion—Monitoring client satisfaction and APO performance

6.57 The APO has established a Client Service Charter that outlines service standards and has developed a series of supplementary brochures that provide information to clients on their rights and responsibilities. Client feedback is collected through the Mystery Shopper Program and APIS. At the time of the audit, there was no centralised collection or analysis of feedback across the APO's office network. However, the APO advised that it is developing a new feedback policy to identify and share better practice and lessons learned across the network.

6.58 The APO consistently meets its target of issuing passports within 10 working days and was able to maintain its performance against this target during the introduction of the ePassport in 2005–06. However, there are opportunities to develop a broader range of quantitative and qualitative indicators for assessing passport integrity and performance for its Annual Report and for reporting on the performance of the FR system to the Senior Executive. In response, the APO has agreed to establish a broader range of indicators to monitor performance.



Ian McPhee

Auditor-General

Canberra ACT

22 May 2012

Appendices

Appendix 1: Agency Response



Australian Government
Department of Foreign Affairs and Trade

4 MAY 2012

Secretary

Telephone: 02 6261 2472
Facsimile: 02 6273 2081

File Number: 11/16338

4 May 2012

Ms Barbara Cass
Group Executive Director
Performance Audit Service Group
Australian National Audit Office
GPO Box 706
CANBERRA ACT 2601



Dear Ms Cass

I refer to your letter of 5 April 2012 and the proposed report on the ANAO's performance audit of the management of ePassports. I note your advice that DFAT's comments will be included in the report.

DFAT welcomes the findings of the report, particularly ANAO's acknowledgement of the new and challenging nature of implementing and managing biometric technology by passport issuing authorities. Australia was instrumental in the development of the international standards for the ePassport and in 2005 was one of the first countries to introduce a compliant ePassport.

I am pleased that the report acknowledges that the Australian Passport Office (APO) has effectively implemented biometric technology and met international ePassport requirements. The report also confirms that the ePassport's electronic security measures, combined with the booklet's security features make the task of producing a fraudulent passport significantly more complex. DFAT appreciates the ANAO assessment that there is a mature and appropriate relationship between APO and its key stakeholders.

DFAT agrees with ANAO's finding that, while not an international requirement, DFAT has incorporated the facial recognition capability to improve identity verification and reduce the incidence of passport fraud.

The report acknowledges that the APO has been responsive to the issues raised during the audit and recognises the measures already undertaken by the APO to

R G Casey Building, Barton ACT 0221 www.dfat.gov.au

implement the suggestions and recommendations in this report. DFAT considers the report's two recommendations to be constructive in identifying opportunities to strengthen the ePassport program.

Comments on Recommendation 1

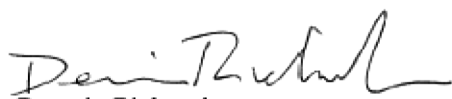
DFAT agrees with this recommendation. DFAT has developed a Future Directions Plan and established a Biometrics Goods and Services Panel to take forward the outstanding issues identified in the 2008 review of its facial recognition system.

Comments on Recommendation 2

DFAT agrees with this recommendation. DFAT welcomes the ongoing involvement of the Defence Signals Directorate (DSD) in our ePassport program. We have commenced work with DSD on a vulnerability assessment project that will examine APO's implementation and integration of the Public Key Infrastructure (PKI). DSD has indicated a willingness to work with APO on future ePassport matters.

I would like to express my appreciation for the constructive approach taken by ANAO throughout the performance of this audit.

Yours sincerely



Dennis Richardson

Appendix 2: Passport timeline

2002	<p>May—DFAT allocated \$3m to conduct research into biometric identifiers for passports.</p> <p>May—USA Visa Waiver Program countries required to implement ePassports by 26 October 2004. The deadline was extended twice, with a final deadline of 26 October 2006.</p>
2003	<p>May—DFAT allocated additional \$3m to continue research into biometric identifiers for passports.</p> <p>June—ICAO adopts the face as the primary biometric identifier for ePassports.</p> <p>November—DFAT launched the 'M' series passport (without microchip).</p>
2004	<p>May—DFAT allocated \$2.2m for the trial of the ePassport.</p>
2005	<p>May—DFAT allocated \$67.5m to implement ePassports.</p> <p>July—Passports Act modernised with increased penalties for passport fraud.</p> <p>October—DFAT launched the 'M' series ePassport and incorporated FR checking into its passport issuing process.</p>
2006	<p>May—DFAT allocated \$14.6m over four years to enhance the security of the passport issuing process.</p> <p>July—APO established as a separate Division of DFAT led by an SES Level 2 Officer.</p> <p>October—Final deadline for countries participating in the USA's Visa Waiver Program to issue their citizens with ePassports.</p>
2007	<p>March—ICAO established the Public Key Directory to collect and distribute PKI certificates.</p> <p>August—Customs and Border Protection commences roll-out of SmartGate, starting with Brisbane International Airport in August 2007, and ending with Darwin International Airport in May 2011.</p>
2008	<p>November—A review of DFAT's FR system is completed.</p>
2009	<p>May—DFAT launched the 'N' series ePassport, which included Active Authentication and enhanced physical security features.</p>
2010	<p>May—DFAT allocated \$100.8m for the Passport Redevelopment Program.</p> <p>From 2010—Work commenced on the design of the 'P' series passport, which is due to be launched in 2014.</p>

Appendix 3: Passport issuing process

APPLICATION

The client completes a passport application form and lodges it in person at an Australia Post outlet, together with supporting documentation.

The applicant must present original proof-of-identity documents such as an Australian birth certificate or Australian citizenship certificate, and other documents such as a driver's licence and Medicare card.

In addition, the applicant must provide two colour photos, with one signed as a true photo by the applicant's guarantor. The guarantor must also provide their details on the application form.



INTERVIEW

A face-to-face interview is held with the applicant to check that the application form has been correctly completed, collect the application fee, check the applicant's photo against ICAO specifications, confirm the applicant's photo resembles the applicant, and sight original proof-of-identity documents and the applicant's current passport.

Australia Post conducts about 85 per cent of all passport interviews on behalf of the APO.



DATA CAPTURE

Applications are passed to the APO and sorted into groups such as priority applications and renewals. Applications are then scanned to capture a black and white image of the application form, and a colour image of the photo and signature.

Data verification then takes place and involves an operator confirming that the Optical Character Recognition program has correctly read each character printed on the original application form, making manual corrections as necessary.

The operator also checks that the applicant's photo is of an acceptable standard. If acceptable, the operator crops (trims) the image and manipulates the photo quality to produce an acceptable image which will appear on the passport booklet.



AUTOMATED ASSESSMENT/FR PROCESSING

APO systems conduct checks against the application form, cross-referencing the data provided by the client and running checks against a number of databases such as citizenship records, and registers of births, deaths and marriages. At the time of the audit, the APO conducted about 200 checks to assess an applicant's eligibility and validate supporting information. This has increased from about 150 checks in 2003.¹⁰²

With the introduction of ePassports in October 2005, the APO introduced an additional eligibility check to reduce the incidence of passport fraud. Using FR technology, the image provided by the applicant is also matched against images held by the APO in the passport database, and against images from Australian travel documents that the applicant previously held. It is also checked against a pending/watchlist database which holds current applications (not yet enrolled in the FR system) and 'persons of interest'.



¹⁰² ANAO Audit Report No.37 of 2002–03, *Passport Services*, p. 69.

ELIGIBILITY PROCESSING

APO Eligibility Officers assess the applicant's eligibility for a passport, and are required to resolve all questions that arise during the automated checks. This is the second formal quality control check—it allows Eligibility Officers to identify and correct any biographical errors prior to the document printing.

The Eligibility Officer also reviews any potential matches made during the FR check (these are presented to them in a gallery). Where an Eligibility Officer suspects fraud, they are required to discuss the matter with more senior officers and/or refer it to the Passport Fraud Section for investigation.



PRINTING AND DISPATCH

The applicant's biographical details are printed onto the passport booklet and a clear plastic laminate is applied to the biographical data page. Biographical data is also written to the microchip embedded in the centre pages of the ePassport.

When the processing of a travel document has been completed, a final check of the physical document, microchip and the biographical details is conducted.

The travel document is then 'dispatched' via Australia Post or courier, or held for collection by the applicant.



FR ENROLMENT

Once the passport has been issued, the applicant's facial image is enrolled into the FR system to enable other facial images to be matched against it.

Note: Steps involving the use of FR technology are highlighted in grey.

Source: ANAO analysis of APO data.

Index

A

Audit

- conclusion, 15
- methodology, 34
- objective, 15, 33
- report structure, 35

Australian Passport Office

- availability of microchip readers, 98–99
- locations, 28
- staff numbers, 13, 28

C

- Clients—satisfaction of, 15, 22, 34–35, 87, 95, 103

D

- Defence Signals Directorate, 16, 21, 22–23, 77, 78, 80, 91–92, 94–95
- DFAT response, 23, 59, 95

E

ePassport security features

- Active Authentication, 74, 78, 109
- Basic Access Control, 37, 74–75, 90
- Passive Authentication, 74, 76–78
- Public Key Infrastructure, 8–9, 37, 39, 40, 43, 74, 76, 78–79, 90, 95, 109

ePassports

- Australian introduction, 14–15, 30, 37, 40
- international requirements, 15, 17, 19, 22, 33, 35–36, 39, 40, 59
- issuing process, 13–14, 16, 18, 28–29, 33, 35, 40, 47–48, 55, 57–58, 65, 69, 70, 109–110

F

Facial recognition

- matching, 9, 14, 16, 18, 19–20, 22, 32–33, 35, 45, 47–48, 50–51, 54, 57, 59–61, 63–65, 67, 69–72, 93, 102
- training and guidance, 16, 19, 61, 63–64

M

- Microchip—robustness, 21, 87–88, 94

P

- Passport fraud, 14, 16, 18, 20–22, 33–35, 40, 42, 45, 47, 51, 61–62, 65–72, 93–94, 100, 101–102, 109–111
- Passport Issue and Control System (PICS), 8, 20, 44, 83–85
- Passport photograph
 - guidance, 55
 - image quality, 19, 54–59
- Passport Redevelopment Program, 13, 19, 20, 29, 58, 62, 68, 72, 93, 109
- Performance information, 17, 22, 69, 95, 97, 99, 100–103
- Privacy—Commissioner, 20, 35, 74–75, 81–82, 85
- Privacy—impacts, 81–82

R

- Risk management, 17, 21, 35, 87, 93–94

U

- USA's Visa Waiver Program, 14–15, 17, 30, 36–40, 109

V

- Vulnerability—monitoring and testing, 9, 17, 21–23, 35, 74, 76, 78–80, 87, 90–92, 94–95

Series Titles

ANAO Audit Report No.1 2011–12

The Australian Defence Force's Mechanisms for Learning from Operational Activities
Department of Defence

ANAO Audit Report No.2 2011–12

Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2010 Compliance)

ANAO Audit Report No.3 2011–12

Therapeutic Goods Regulation: Complementary Medicines
Department of Health and Ageing

ANAO Audit Report No.4 2011–12

Indigenous Employment in Government Service Delivery

ANAO Audit Report No.5 2011–12

Development and Implementation of Key Performance Indicators to Support the Outcomes and Programs Framework

ANAO Audit Report No.6 2011–12

Fair Work Education and Information Program
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.7 2011–12

Establishment, Implementation and Administration of the Infrastructure Employment Projects Stream of the Jobs Fund
Department of Infrastructure and Transport

ANAO Audit Report No.8 2011–12

The National Blood Authority's Management of the National Blood Supply
National Blood Authority

ANAO Audit Report No.9 2011–12

Indigenous Secondary Student Accommodation Initiatives
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.10 2011–12

Administration of the National Partnership on Early Childhood Education

Department of Education, Employment and Workplace Relations

ANAO Audit Report No.11 2011–12

Implementation and Management of the Housing Affordability Fund

Department of Families, Housing, Community Services and Indigenous Affairs

Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.12 2011–12

Implementation of the National Partnership Agreement on Remote Indigenous Housing in the Northern Territory

Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.13 2011–12

Tasmanian Freight Equalisation Scheme

Department of Infrastructure and Transport

Department of Human Services

ANAO Audit Report No.14 2011–12

Indigenous Protected Areas

Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.15 2011–12

Risk Management in the Processing of Sea and Air Cargo Imports

Australian Customs and Border Protection Service

ANAO Audit Report No.16 2011–12

The Management of Compliance in the Small to Medium Enterprises Market

Australian Taxation Office

ANAO Audit Report No.17 2011–12

Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2011

ANAO Audit Report No.18 2011–12

Information and Communications Technology Security: Management of Portable Storage Devices

ANAO Audit Report No.19 2011–12

Oversight and Management of Defence's Information and Communication Technology
Department of Defence

ANAO Audit Report No.20 2011–12

2010–11 Major Projects Report
Defence Materiel Organisation

ANAO Audit Report No.21 2011–12

Administration of Grant Reporting Obligations
Department of Finance and Deregulation

ANAO Audit Report No.22 2011–12

Administration of the Gateway Review Process
Department of Finance and Deregulation

ANAO Audit Report No.23 2011–12

Administration of the National Greenhouse and Energy Reporting Scheme
Department of Climate Change and Energy Efficiency

ANAO Audit Report No.24 2011–12

*Administration of Government Advertising Arrangements:
March 2010 to August 2011*

ANAO Audit Report No.25 2011–12

Administration of Project Wickenby
Australian Taxation Office
Australian Crime Commission
Australian Federal Police

ANAO Audit Report No.26 2011–12

Capacity Development for Indigenous Service Delivery
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Education, Employment, and Workplace Relations
Department of Health and Ageing

ANAO Audit Report No.27 2011–12

Establishment, Implementation and Administration of the Bike Paths Component of the Local Jobs Stream of the Jobs Fund

Department of Regional Australia, Local Government, Arts and Sport
Department of Infrastructure and Transport

ANAO Audit Report No.28 2011–12

Quality On Line Control for Centrelink Payments

Department of Human Services

ANAO Audit Report No.29 2011–12

Administration of the Australia Network Tender Process

Department of Foreign Affairs and Trade
Department of Broadband, Communications and the Digital Economy
Department of the Prime Minister and Cabinet

ANAO Audit Report No.30 2011–12

Fighting Terrorism at its Source

Australian Federal Police

ANAO Audit Report No.31 2011–12

Establishment and Use of Procurement Panels

Australian Securities and Investments Commission
Department of Broadband, Communications and the Digital Economy
Department of Foreign Affairs and Trade

ANAO Audit Report No.32 2011–12

Management of Complaints and Other Feedback by the Department of Veterans' Affairs

Department of Veterans' Affairs

Current Better Practice Guides

The following Better Practice Guides are available on the ANAO website.

Environmental Sustainability in Australian Government Operations	Apr 2012
Developing and Managing Contracts – Getting the right outcome, achieving value for money	Feb 2012
Public Sector Audit Committees	Aug 2011
Human Resource Information Systems Risks and Controls	Mar 2011
Fraud Control in Australian Government Entities	Mar 2011
Strategic and Operational Management of Assets by Public Sector Entities – Delivering agreed outcomes through an efficient and optimal asset base	Sep 2010
Implementing Better Practice Grants Administration	Jun 2010
Planning and Approving Projects an Executive Perspective	Jun 2010
Innovation in the Public Sector Enabling Better Performance, Driving New Directions	Dec 2009
SAP ECC 6.0 Security and Control	Jun 2009
Preparation of Financial Statements by Public Sector Entities	Jun 2009
Business Continuity Management Building resilience in public sector entities	Jun 2009
Developing and Managing Internal Budgets	Jun 2008
Agency Management of Parliamentary Workflow	May 2008
Public Sector Internal Audit An Investment in Assurance and Business Improvement	Sep 2007
Fairness and Transparency in Purchasing Decisions Probity in Australian Government Procurement	Aug 2007
Administering Regulation	Mar 2007
Developing and Managing Contracts Getting the Right Outcome, Paying the Right Price	Feb 2007
Implementation of Programme and Policy Initiatives: Making implementation matter	Oct 2006

