The Auditor-General
Audit Report No.24 2007–08
Performance Audit

DIAC's Management of the Introduction of Biometric Technologies

Department of Immigration and Citizenship

Australian National Audit Office

© Commonwealth
of Australia 2008

ISSN 1036–7632

ISBN 0 642 81004 4

COPYRIGHT INFORMATION

Australian National
Audit Office

Canberra ACT
26 February 2007

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in the Department of Immigration and Citizenship in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit and the accompanying brochure. The report is titled *DIAC's Management of the Introduction of Biometric Technologies.*

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 Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

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

Tom Clarke
Celine Roach
Susan Murray
Edwin Apoderado
Matthew Plum
Anne Martin
Peter White

Contents

Tables

Figures

Abbreviations

ACS	Australian Customs Service
AFP	Australian Federal Police
BSD	Border Security Division
CIU	Cabinet Implementation Unit
CoBIT	Control Objectives for Information and Related Technology
CRF	Consolidated Revenue Fund
DAON	Department of Immigration and Citizenship software
DCR	Detention Centre Rollout
DFAT	Department of Foreign Affairs and Trade
DIAC	Department of Immigration and Citizenship
DIMIA	Department of Immigration and Multicultural and Indigenous Affairs. On 27 January 2006, the office of Indigenous Policy Coordination moved to the Department of Family, Community Services and Indigenous Affairs.
DNA	Deoxyribonucleic acid (contains the genetic instructions found in all known living organisms)
DSTO	Defence Science and Technology Organisation
GEM	Governance, Evaluation and Monitoring
ICAO	International Civil Aviation Organisation
ICSE	Integrated Client Services Environment
IDC	Inter-departmental Committee
IPPs	Information Privacy Principles

IRC	Identity Resolution Centre
IRIS	Immigration Records Information System
ISR	Identity Services Repository
IT	Information Technology
ITPO	IT Programme Office
LEGEND	A DIAC system through which the departmental staff can access the Procedures Advice Manual.
MAL	Movement Alert List
MoU	Memorandum of Understanding
MRTD	Machine Readable Travel Document
MSIs	Migration Series Instructions
NAFIS	National Automated Fingerprint Identification System
NIVA	National Identity Verification and Advice
NPP	New Policy Proposal
OPC	Office of the Privacy Commissioner
PAM	Procedures Advice Manual
PM & C	Department of Prime Minister and Cabinet
PMBOK	Project Management Body of Knowledge
RAPIDS	DIAC software
RDA	Records Disposal Authority
RFID	Radio Frequency Identification
SAU	Strategic Assessment Unit

SDLC	Software Development Life-cycle
SfP	Systems for People
SRO	Senior Responsible Officer
UK	United Kingdom
US/USA	United States of America
VAC	Visa Application Charge
VWP	Visa Waiver Programme

Summary and Recommendations

Summary

Introduction

1. The Department of Immigration and Citizenship (DIAC) employs more than 7000 staff, located in offices around Australia and overseas.[1] DIAC's key tasks include: entry, stay and departure arrangements for non-citizens; migrant and humanitarian settlement arrangements; border (immigration) control and security; citizenship; and ethnic and multicultural affairs.[2] In undertaking these tasks, DIAC exercises powers under a range of immigration and citizenship legislation, chiefly, the *Migration Act 1958* and the *Australian Citizenship Act 2007*.[3]

2. DIAC and other Australian Government agencies with roles in border security have been considering the potential benefits for using 'biometrics' since the late 1990s to assist them in discharging their responsibilities. The term 'biometrics' describes information drawn from a person's characteristics that is relatively unique and relatively invariant (unchanging). A person's biometric information can assist in *identifying* the person and/or *verifying* their claimed identity. The technology behind biometrics, and its associated standards, is evolving rapidly.

3. From 2003, DIAC, the Australian Customs Service (ACS), the Department of Foreign Affairs and Trade (DFAT), and the Office of the Privacy Commissioner (OPC) started developing a four-agency approach to the introduction of biometrics for border control. Under the four-agency *Biometrics for Border Control* initiative, DIAC has been funded to undertake a number of inter-related projects.

4. The benefits of biometrics in the area of border security generally relate to reduced rates, and financial impacts, of identity fraud, improved confidence in administration and national security, and greater efficiency in border processing. Some of these benefits, and their associated costs, are difficult to quantify.

5. After the announcement of the introduction of the *Biometrics for Border Control* initiative (May 2005), the Government announced substantial

[1] Department of Immigration and Multicultural Affairs, *Portfolio Budget Statements 2007–08*, pp. 49, 71.

[2] ibid., p. 26.

[3] On 1 July 2007, the *Australian Citizenship Act 2007* replaced the *Australian Citizenship Act 1948*.

administrative and systems reform for DIAC in response to the Palmer and Comrie Reports.[4] Funding of $231 million over four years was announced in October 2005 for what became known as the 'Palmer Implementation Plan'.[5]

6. Results of a DIAC review of its information requirements and systems gave rise to the 'Systems for People' initiative announced in May 2006 ($495 million over four years).[6] Both the Palmer Implementation Plan and Systems for People changes post-date DIAC's biometrics program, but have direct and indirect influences on the biometrics projects. Notwithstanding the substantial additional funding provided to the department, DIAC has found its overall budget position to be challenging, with the resulting management responses impacting on individual projects and program areas.

7. A contractor was selected as DIAC's strategic biometrics partner to provide a suite of biometric solutions, software tools and a range of identity management services, including research. At the time of the audit, two system development projects were underway, the Identity Services Repository (ISR) and the Detention Centre Rollout (DCR).

8. The ISR project, which commenced in mid-2004 and is ongoing, provides the basis for a consistent approach to the management of client identity information held by DIAC. The DCR project was introduced to acquire, store, retrieve and match biometric data, and deliver the infrastructure and training to support the introduction of biometric systems in detention facilities and its compliance operations. [7]

Audit scope and objective

9. The audit objective was to determine whether DIAC's biometrics program had appropriate:

- business review processes (including a business case);
- authorisation;

[4] DIMIA, September 2005, *Report from the Secretary to Senator the Hon Amanda Vanstone Minister for Immigration and Multicultural and Indigenous Affairs: Implementation of the Recommendations of the Palmer Report on the Inquiry into the Circumstances of the Immigration Detention of Cornelia Rau.* See also Amanda Vanstone, Minister for Immigration and Multicultural Affairs, 6 October 2005, *Palmer Implementation Plan and Comrie Report*.

[5] MJ Palmer, op. cit, 2005; and Commonwealth Ombudsman, op. cit, 2005.

[6] Amanda Vanstone, Minister for Immigration and Multicultural Affairs media release, 9 May 2006, *Palmer and Comrie Reports Guide DIMA's Budget*.

[7] DIAC, 2007, *Detention Centre Rollout of Biometrics—IT Project Management Plan*, Version: 2.0.

- business and IT governance arrangements; and
- IT project management and systems development arrangements.

10. The audit scope was on the design and planning for the introduction of biometrics in DIAC. Matters concerning the implementation of the technology in DIAC and arrangements with other agencies in relation to the '*Biometrics for Border Control*' initiative were outside the audit scope.

Overall audit conclusion

11. Better verification of claimed identity, and identification of persons where there may be doubt about their identity, are priorities for the Australian Government, as is the appropriate protection of individual privacy. DIAC's introduction of biometric technologies is an important part of its response to these priorities. Total funding for the biometrics initiatives amounts to more than $83 million over the period 2003–04 to 2009–10.

12. DIAC's introduction of biometric technologies has been challenging given the rapidly evolving nature of the technologies involved and the dynamic international environment in which the technology is being deployed. The DIAC biometrics program area has also had to adapt to substantial changes to the internal DIAC systems environment during the design and deployment phase of the program. Consequently, there have been delays in the delivery of planned biometric capabilities.

13. Consistent with the approach taken by ACS and DFAT, DIAC has chosen the facial image as its primary biometric and has invested its resources accordingly. However, its main overseas counterpart agencies (in the USA and UK) have subsequently begun implementing multi-modal biometric systems, involving both facial images and fingerprints. DIAC's current relatively limited capability to use other biometric data, such as fingerprints, raises the risk that it will not be in a position to benefit fully from the international developments tending towards a broader use of fingerprints, particularly in enabling effective matching for watch–list and other identification purposes.

14. DIAC obtained a clear government mandate to research and conduct detailed tests and trials of potential biometric technology options and, subsequently, to introduce the technologies. Accompanying legislation has been put in place. The legislation is due to be reviewed during 2008, and the ANAO identified additional areas for consideration during the review. In particular, the consistency between legislative wording and policy intent

relating to the assessment of personal identifiers (which include biometric information), and the provisions relating to retaining and destroying personal identifiers would benefit from review.

15. DIAC's planning for the introduction of biometrics, including its business case, was generally sound. DIAC's planning documents established clear timelines and adequate review points. The business case identified reasons for, and the expected benefits and costs that could accrue from, introducing biometrics. However, the ANAO concluded that DIAC would benefit from a more structured approach to monitoring changes arising from its introduction of biometrics over time and evaluating the effectiveness of its chosen biometric solution in delivering its expected benefits. This is necessary to support management decisions about future directions in this area.

16. DIAC has in place strong provisions in legislation aimed at protecting sensitive personal information, including biometric information. However, while the framework is sound, the ANAO concluded that DIAC needs to strengthen substantially its processes for assuring itself that the legislative requirements in relation to access, disclosure, retention and destruction of personal identifiers and related information are being implemented consistently and appropriately.

17. DIAC's business governance arrangements for the introduction of biometric technologies were sound. However, the ANAO identified a number of lessons for DIAC to consider, both in terms of future biometric project activity, and more generally. These lessons included:

- ensuring that key meetings and decisions including the assessment of projects risks, are appropriately documented;
- ensuring that there is shared understanding among stakeholders about the allocation of funds to projects and that systems accurately record both project allocations and expenditures;
- involving DIAC's Internal Audit in IT system development initiatives;
- ensuring compliance with DIAC's IT project management framework; and
- implementing DIAC's requirements management mechanism for the biometrics projects. This would assist DIAC in capturing and managing system features and functions that are required to meet the needs of business stakeholders.

Key findings

Planning for Implementation (Chapter 2)

18. In 2004 DIAC was authorised to research and test ways of incorporating biometric technologies into existing visa and entry arrangements, and a capacity to store biometric images. The funding was for twelve months and was followed by a four-year initiative known as the *Biometrics for Border Control* initiative in 2005.

19. In considering its options for introducing biometrics, DIAC had conducted several tests and trials of biometric technologies. The Defence Science and Technology Organisation provided analyses into the effects associated with biometric enrolment and verification on DIAC.

20. In 2005, DIAC prepared a business case that identified sound reasons why a phased application of biometrics should be approved. Alternative non-biometric options to introducing biometrics were explored in earlier DIAC work but were not addressed in the business case. The scope and requirements were also apparent in the business case, but did not include a clear timeframe for the project development.

21. Also in 2005, DIAC prepared a cost-benefit analysis as part of the *Biometrics for Border Control* initiative and later identified key benefits to government from the introduction of biometrics. The expected benefits and costs are assessable, but to be meaningful, DIAC would benefit from a more structured approach to monitoring changes arising from its introduction of biometrics over time and evaluating the effectiveness of its chosen biometric solution in delivering its expected benefits. This is necessary to support management decisions about future directions in this area. DIAC's recently established evaluation and monitoring team is a useful first step in establishing an effective monitoring and evaluation capability.

22. A number of planning documents have also been prepared. Aside from a cross-agency Implementation Plan, DIAC also developed its own Implementation and Strategic Plans for the introduction of biometrics.

23. Success factors and critical dependencies were clearly identified in DIAC's planning documents. DIAC established clear timelines that set adequate review points for both business and IT deliverables. However, there have been delays in the delivery of specific capabilities primarily as a consequence of unmet dependencies on other related biometric or IT projects.

24. The wording of the *Migration Act 1958* expects DIAC decision makers to form judgements about the qualities ('integrity') of personal identifiers provided by DIAC clients. However, DIAC's policy guidance indicates that the intention was not that the qualities of personal identifiers themselves should be assessed, but rather that assessment should be of the *claims* being made by people about the identifiers (that the personal identifiers are theirs). In such a contestable area, there would be merit in DIAC considering the consistency between the legislation, as drafted, and the policy intent as part of a review of the legislation scheduled for 2008.

25. In approving the *Biometrics for Border Control* initiative, the Government decided that the four agencies should give priority to ensuring that the biometric technology introduced is fully interoperable with similar technology developed by other countries. Consistent with the approach taken by ACS and DFAT, DIAC has chosen the facial image as its primary biometric and has invested its resources accordingly. Its main counterpart overseas agencies (USA and UK) are implementing multi-modal biometric systems, involving faces and fingerprints.

26. Currently, DIAC has relatively limited capability to use other biometric data, such as fingerprints for matching purposes. Consequently, there is a risk that DIAC is unable to benefit fully from interactions with domestic and overseas systems. DIAC's early strategies have mainly focused on the use of face as a one-to-one matching capability. The current relatively limited fingerprint matching capability leaves the department in a position where it is unable to benefit fully from the international developments tending towards a broader use of fingerprints.

27. To maximise interactions with domestic and overseas systems, particularly in enabling effective matching for watch list and other identification purposes, DIAC should assess the costs and benefits of broadening its biometric capability.

Governance Arrangements (Chapter 3)

28. The four agencies involved in the *Biometrics for Border Control* initiative developed a governance model aimed at ensuring cross-agency outputs supporting whole of government objectives were met, and individual agency objectives aligned with the whole of government framework. Similarly, DIAC's Identity Branch introduced new governance arrangements to ensure

alignment with broader DIAC planning processes and its strategic plan for identity management.

29. DIAC's Identity Branch has responsibility for the agency's implementation of identity management solutions, including biometrics. The Branch's current organisational framework aligns and integrates the individual projects to the rest of the department. There are clear accountability arrangements within the Branch.

30. DIAC's current IT governance structure was introduced in late 2005. Systems Boards are responsible for overseeing specific systems within their defined areas. All IT governance bodies advise and report to DIAC's Systems Committee. DIAC's highly rated IT risks were reported to DIAC's Systems Executive Board. However, there were limited details recorded of specific risks in relation to biometric IT projects discussed in meetings of DIAC's Border Systems Board.

31. DIAC's biometric related IT projects, the Identity Services Repository (ISR) and the Detention Centre Rollout (DCR) projects, report through the IT governance structure. Both the ISR and DCR projects were providing project status information, as required by the DIAC IT project management framework. However, more comprehensive documentation of key decisions, and reasons for the decisions would strengthen project design and administration. DIAC's Internal Audit has had little involvement in the development of the biometric systems.

32. At the time of the audit, there was uncertainty in DIAC's Identity Branch about the allocation of funds to the biometrics projects—however this was clarified as a result of the audit. While it is possible to report on aggregate allocations and expenditure for the biometrics projects, DIAC's practices in recording project level expenditure were inadequate, meaning that any project-level reporting for the $83 million biometrics projects is likely to be substantially inaccurate. Going forward, the ANAO considers that more transparent and timely communication of allocation decisions and better data on project expenditures would help in managing the biometrics projects and in accounting for the use of funds approved by government for DIAC's biometrics initiatives.

33. The goal of offsetting the costs of the biometrics initiatives by raising the Visa Application Charge (VAC) by five per cent on certain visa types could have been better managed and monitored. The ANAO found that there is likely to be substantially more revenue raised than originally projected─in

essence a ‘windfall’ gain to the Australian Government. Closer monitoring would have helped the department to better manage the risks of not meeting the Government’s intention to ‘offset’ the costs of the program through the VAC increase.

Administrative Arrangements (Chapter 4)

34. DIAC has prepared detailed draft guidance and adequate training on client identity matters, including biometrics. Although the guidance is sound its finalisation has not been timely. There have also been delays in up-loading the completed guidance onto LEGEND (the system through which DIAC staff can access policy guidance).

35. When the guidance is completed and is made available for staff, it would benefit from being accompanied by a performance monitoring and feedback strategy. DIAC’s national Quality Assurance Framework may provide a suitable platform for obtaining this assurance.

36. DIAC has also prepared an Identity Management Training Plan 2007–2010, that maps out sound training initiatives for the Identity Branch.

37. In order to assure information privacy, DIAC designed its ISR so that access is based on a person’s ‘position number’. However, DIAC was unable to provide evidence of actions taken to ensure that access to identifying information was only by authorised officers. Further, there was no monitoring process to provide assurance about the appropriateness of access to identifying information by authorised officers.

38. Protections in the *Migration Act 1958* surrounding access to, and disclosure of, identifying information do not extend to third parties to which DIAC discloses information. DIAC cannot ensure that there is/will be no inappropriate use or disclosure of identifying information by the agencies to which it discloses the information. Stronger provisions in DIAC’s Memoranda of Understanding would provide some further assurance that identifying information disclosed by DIAC to third parties is appropriately protected. There is also no effective process to provide assurance that disclosures of identifying information by DIAC officers are appropriately documented.

39. While there is a general legislative requirement to destroy identifying information, there are exceptions. These exceptions mean that DIAC is

authorised to retain indefinitely virtually all of the biometric information it is currently planning to collect.[8]

40. DIAC's current Records Disposal Authority (RDA) provides for the disposal of records one year after 'the action is completed'. DIAC advised that it was 'looking at ensuring that dates of entry of data are flagged'. Although this will be a useful first step, DIAC needs to institute monitoring processes to identify aged information for destruction and should consider whether the legislative provisions with respect to the retention and destruction of identifying information are functioning fully as intended.

41. DIAC is in the process of implementing an IT system development framework that can support DIAC's current and future biometric software development activities. However, given the relative immaturity of the framework and tools, the ANAO was not in a position to assess its implementation.

42. As required by the Systems for People program, software development and release management process have been implemented for two of DIAC's biometric system development projects that are currently underway, the ISR and DCR projects.

43. However, for the DCR project, system development documents were not being formally reviewed or approved by all business stakeholders and groups involved in developing the system. This is essential for quality assurance.

44. DIAC has not implemented its requirements management mechanism for its biometrics related IT projects. The absence of an effectively implemented requirements management mechanism raises risks that DIAC's biometric related system will be completed without all the originally specified features and functions, or that the features and functions implemented may not meet the needs of business stakeholders.[9] The ANAO found evidence of these risks eventuating.

[8] Information such as biometric photographs from a range of visa and citizenship applicants, as well as fingerprints of people in immigration detention.

[9] Consequential risks include: the system may not be accepted by the business stakeholders; compensating manual processes may need to be introduced (which will have associated costs, risks and inefficiencies); and further system re-development effort may be needed at an additional cost to address shortcomings in features and functions of the system.

Recommendations

45. The ANAO has made four recommendations and a number of suggestions to strengthen DIAC's management of the introduction of biometric technologies. DIAC agreed with all four recommendations.

DIAC response to the audit

46. DIAC welcomes the audit into the introduction of biometric technology, which has made constructive recommendations that will enable the department to better manage, measure and assess the benefits of the biometric solutions being implemented. DIAC's identity management strategy is a complex, multi-faceted programme of work in a dynamic environment, requiring national and international collaboration as well as a whole of agency change management agenda. It is fundamentally important that we maximize the benefits from our identity management and biometric tools and continue to balance our roles of facilitating genuine travel while deterring those who would circumvent our visa and border systems.

47. The ANAO's findings in relation to the department's sound business governance and planning for the introduction of biometrics are pleasing, and the audit recommendations will help the department to capitalise on this through improved assurance mechanisms. The audit will assist DIAC to build on the lessons learned to date and will contribute to the department's capability to effectively identify those entering Australia and to maintain that foundation identity for use within the Australian community.

Recommendations

Set out below are the ANAO's recommendations which aim to strengthen DIAC's management of the introduction of biometric technologies. Report paragraph references and abbreviated responses from DIAC are included.

Recommendation No.1

Para 2.81

The ANAO recommends that, in order to support management decisions about future directions, DIAC implements a structured approach to monitoring changes arising from the introduction of biometrics over time, and evaluating the effectiveness of its chosen biometric solution in delivering its expected benefits.

DIAC response: *Agree.*

Recommendation No.2

Para 2.83

The ANAO recommends that, in order to maximise potential for interoperability with overseas countries and Australian agencies and enable effective matching for watch-list and other identification purposes, DIAC assesses the costs and benefits of broadening its biometric capability to make more use of the main types of available data, including facial images and fingerprints.

DIAC response: *Agree.*

Recommendation No.3

Para 4.67

The ANAO recommends that, consistent with the direction taken in its National Quality Assurance Framework, DIAC:

- obtains structured feedback from decision makers on the usefulness of operational policy guidance relating to biometrics, and develops a means for obtaining assurance that decision makers are implementing the policy guidance consistently and appropriately; and
- strengthens its processes for obtaining assurance that the legislative requirements in relation to access, disclosure, retention and destruction of personal identifiers and related information are implemented consistently and appropriately.

DIAC response: *Agree.*

Recommendation No.4

Para 4.69

The ANAO recommends that, in order to strengthen quality assurance for the development of IT systems, DIAC ensures that system development documents are reviewed and approved by business stakeholders and groups involved in developing these systems, and its requirements management mechanism is implemented for biometrics projects.

DIAC response: *Agree.*

Audit Findings and Conclusions

1. Background and Context

This chapter provides background and context to DIAC's introduction of biometrics.

Introduction

1.1 The Department of Immigration and Citizenship (DIAC) employs more than 7000 staff, located in offices around Australia and overseas.[10] Projected resources in 2007–08 for DIAC is around $1626 million.[11]

1.2 DIAC seeks to 'enrich Australia through the well-managed entry and settlement of people'.[12] Key tasks include: entry, stay and departure arrangements for non-citizens; migrant and humanitarian settlement arrangements; border (immigration) control and security; citizenship; and ethnic and multicultural affairs.[13] In undertaking these tasks, DIAC exercises powers under a range of immigration and citizenship legislation, chiefly, the *Migration Act 1958* and the *Australian Citizenship Act 2007*.[14]

What are 'biometrics'?

1.3 The term 'biometrics' describes information drawn from a person's characteristics that is relatively unique and relatively invariant (unchanging). A person's biometric information can assist in:

- *identifying* the person, for example, when 'one-to-many' comparisons are made between the biometric data taken from the person with biometric data held in a database; and/or
- *verifying* their claimed identity, for example, when 'one-to-one' comparisons are made between the biometric data taken from the person with biometric data for their claimed identity held in other authoritative information sources (such as documents or databases).

[10] Department of Immigration and Multicultural Affairs, *Portfolio Budget Statements 2007–08*, pp. 49, 71.

[11] ibid., p. 24.

[12] ibid., p. 19. On 23 January 2007 the Department was renamed having been termed the Department of Immigration and Multicultural Affairs (DIMA) from 27 January 2006, and the Department of Immigration Multicultural and Indigenous Affairs (DIMIA) previously. In this audit the Department's current title is used, except in references and quotations, where the historical title is used.

[13] ibid., p. 26.

[14] On 1 July 2007, the *Australian Citizenship Act 2007* replaced the *Australian Citizenship Act 1948*.

1.4 There are two main types of biometric identifiers: physiological and behavioural.[15] Table 1.1 lists the more common biometric identifiers.

Table 1.1

Different types of biometric identifiers

Characteristic	Biometric Identifier
Physiological	Fingerprint Face Iris Retina Hand geometry Finger/Palm vein DNA
Behavioural	Voice patterns Handwriting/Signature Keystroke dynamics Gait

Source: ANAO.

1.5 The use of biometrics for identity purposes is not new. Fingerprints have long been used to identify persons, while the signature is ubiquitous as evidence of personal authorisation of a document.[16]

1.6 However, the development of technologies[17] that automate the capture of biometric data and comparison of this data with data from other sources is relatively recent.[18] In this audit, the term 'biometrics' is used to encompass both the characteristics being measured and the technology used to capture and compare the biometric data.[19]

[15] Physiological characteristics are inherited traits, such as eyes, face and hands. Behavioural characteristics are learned traits, such as voice patterns, handwriting and typing patterns.

[16] The overwhelming world-wide use of fingerprints is for definitive identity records management purposes.

[17] The technologies use a mathematical formula to determine the extent to which live images match electronically stored images or templates taken from stored images. Before the system can be used to analyse a person, it must have a database record, or template, of that person. The act of capturing a person's biometrics and creating the template is known as 'enrolment'. All biometric technologies must have a template representing each enroled member.

[18] Other sources may include documents containing biometric data and/or databases of biometric data.

[19] Biometrics are intended to supplement or even replace replace manual identity checks and can potentially increase speed, consistency and accuracy of identity checking, and increase confidence about a person's identity. In this instance, biometrics can be used to increase assurance that a person is who they claim to be.

Biometrics are developing rapidly

1.7 The technology behind biometrics and its associated standards are evolving rapidly. Considerable research and development has been, and continues to be, undertaken both domestically and internationally.

1.8 Biometric technologies vary in terms of maturity, accuracy of matching and performance. For example, when comparing facial, fingerprint and iris biometrics in 2004, DIAC considered that:

- fingerprint technology is the most mature and has the highest number of implementations. However, current negative community perceptions linking fingerprints with criminality, must be taken into account;
- iris matching capability is currently the most accurate, however, the provision of this technology is currently limited to one vendor only, creating a monopoly which introduces risks for agencies considering this capability;
- the main issue with facial images is the quality of the images, particularly where third parties are used to take digital photos. Accuracy rates are subject to a range of environmental conditions and implementation of capture standards.[20]

1.9 The accuracy of biometric matching has improved markedly in recent years. For example, in tests sponsored by US Government agencies, current (2006) facial recognition technology showed 'order of magnitude,' or tenfold, improvement in recognition performance over comparable tests conducted in 2002. [21]

Border security agencies' increasing focus on biometrics

International developments

1.10 Internationally, there has been serious focus on the use of biometrics for border security since the late 1990s.[22] Initiatives taken following the terrorist

[20] The department also considered that 'regardless of whether or not facial images are of sufficient quality to use for automated biometric matching, making digital images available on line for human inspection is still assessed to add significant value in combating identity fraud and ensuring consistency of identity.' DIMIA, 2004, *Biometric Steering Committee report – Biometrics Requirements Discovery Project*, p.15. In addition, facial images may be useful at various processing stages in DIAC's work, such as preventing substitution at English Language Testing, Citizenship processes and health assessments.

[21] These tests are managed by the US National Institute of Standards and Technology.

[22] ICAO commenced investigating biometrics, and their potential to enhance identity confirmation in passports in 1997.

attacks of 11 September 2001 in the USA have focused in part on biometrics, as the following example shows.

Example: the introduction of 'e-Passports'

One of the initiatives taken by the US Government to strengthen border security after the terrorist attacks of 11 September 2001, was to develop biometric-enabled passports ('e-Passports') for its citizens and, correspondingly, require that foreign governments issue e-Passports to their citizens as a condition of continued involvement in the US Government's visa waiver programme (VWP).

The 27 States participating in the VWP were required to issue machine readable passports with digitised photos by 26 October 2005 and present a plan to begin issuing passports with integrated circuit chips within one year ('e-Passports').[23]

The International Civil Aviation Organisation (ICAO) adopted the international standard for e-Passports in May 2003.[24] The standard specified the face as the primary biometric, mandatory for global interoperability, and recommended the finger and iris as secondary biometrics to be used at the discretion of the passport-issuing State.[25]

Australia was the fifth country to introduce e-Passports for its citizens (October 2005).[26] After many delays, US e-Passports were introduced in August 2006.

1.11 While the immediate effect of the US Government's actions was to force other governments to change their passports, it also gave impetus to the further development of biometrics in other areas of border security.

1.12 DIAC's overseas counterpart agencies are also introducing biometrics. There is considerable focus on 'multi-modal' biometrics,[27] predominantly fingerprint and facial matching.[28]

[23] See ICAO *MRTD Report* Vol 1 No 1 2006. E-Passports are essentially enhanced versions of existing machine readable passports or Machine Readable Travel Documents (MRTDs). The ICAO sets international standards for the mandatory data items and their form and position for MRTDs. The ICAO specified that the biometric data be stored in a contactless integrated circuit, also known as a radio frequency ID (RFID) chip which would be embedded in the passport. (see: ICAO, Document 9303 *Machine Readable Passports*, and ICAO, *Supplement to Document 9303*.)

[24] ICAO *MRTD Report* Vol 1 No 1 2006, p. 37.

[25] The facial image was chosen as the preferred biometric because it is relatively easy and non-intrusive to capture, it is universal (everyone has a face), and checking can be done manually if the equipment fails.

[26] ICAO *MRTD Report* Vol 2 No 1 2007, p. 43.

[27] In this audit, 'multi-modal' refers to the use of multiple different biometrics such as facial images and fingerprints. On a risk basis, one biometric can be supplemented or replaced with another to enhance identity determination.

[28] Under the US-Visit Program, most travellers to the USA must provide two biometric finger scans and digital photographs at the time of visa application (where necessary) and arrival at the border. In November 2007, the United States will start requiring travellers to the US to give 10 digital fingerprints on arrival. Similarly, the United Kingdom regards fingerprint visas as the 'first line of defence against illegal immigration. The UK government has announced that by April 2008, it will have completed a global roll-out of biometric data collection to all its overseas missions. By 2011, all non-European Economic Area passengers will be required to supply biometrics before travel to UK or on arrival.

Australian border security agencies' approach

1.13 Australian Government agencies with roles in border security have been considering the potential benefits for using biometrics since the late 1990s. For example DIAC has been considering the potential use of biometrics for its business since at least 1999. Similarly, the Australian Customs Service (ACS) has been developing a biometric solution for border clearance, known as 'Smartgate', since February 2001,[29] and the Department of Foreign Affairs and Trade (DFAT), began developing the e-Passport for Australian citizens from 2002–03 (see example above).

1.14 From 2003, the three agencies, together with the Office of the Privacy Commissioner (OPC), started developing a four-agency approach to the introduction of biometrics for border control.

Biometrics for Border Control initiative: ACS, DFAT, DIAC and OPC[30]

In May 2004 DIAC, DFAT, ACS and the OPC received funding from the Government for an initiative known as *Biometrics for Border Control*. The agencies received funding for one year to research and pilot some of the proposed systems. DIAC was allocated $4.4 million to: research and test the best way to incorporate biometric technologies into Australia's existing electronic visa and entry arrangements and to develop a capacity to store and use digital biometric images to better identify its clients each time they deal with the Department.

In May 2005, the same agencies received further funding of $185.75 million over four years (2004–05 to 2007–08). Of this, $42.87 million was for DIAC to implement biometrics for border security and identity verification.[31]

The balance of the funding was for the development of e-Passports by DFAT ($67.53 million)[32] and Smartgate by ACS ($74.6 million),[33] with $0.74 million also being provided to the OPC to provide advice and conduct privacy audits.

DIAC's biometrics projects

1.15 Under the four-agency *Biometrics for Border Control* initiative, DIAC has been funded to undertake a number of inter-related projects. DIAC also

[29] Smartgate was initially designed to compare a live facial image with a pre-enrolled image stored on a central database. As such, its target client group was frequent travellers. The impetus for automation was primarily efficiency, rather than security, although the profile of the latter has since risen.

[30] Also referred to in this audit report as the 'four-agency initiative'.

[31] Visa application charges (excluding tourism, student and visitor visa classes) were increased by five per cent to offset the costs of the new program in DIAC.

[32] The cost was to be offset by a $19 increase in the fee for an adult passport. $8.7 million had been previously committed between 2002–03 and 2004–05 to research and test a prototype e-passport.

[33] The introduction of e-passports changed the direction of the Smartgate project. The system was re-configured to check live images against images stored in an e-Passport.

received funding in May 2006 which included additional biometrics projects.[34] DIAC's biometrics projects are set out in Table 1.2.

Table 1.2

DIAC's biometrics projects 2004–05 to 2009–10

	Projects
Biometrics for Border Control 2004–05 (twelve months)	• Conduct research programs. • Implement an Identity Services Repository (ISR) (the ISR is a database for all information relating to the identity of DIAC clients, including biographic, documents, and biometric information).
Biometrics for Border Control 2005–06 (four years)	• Evaluate, procure and deploy biometric equipment for static and mobile use. • Fully integrate the ISR with existing DIAC systems. • Implement biometric matching, verification and identification. • Collect images across all DIAC business processes using a universal biometric enrolment portal. • Match all images collected against national security alerts. • Link the ISR with the Australian and New Zealand passport databases. • Assess the feasibility of linking biometric information in DIAC and ACS border systems.
Systems for People 2006–07 (four years)	Roll out biometrics to compliance areas as well as detention centres.

Source: ANAO, based on DIAC documents.

Note: Funding for the ISR was transferred from the *Biometrics for Border Control* program to the Systems for People program.

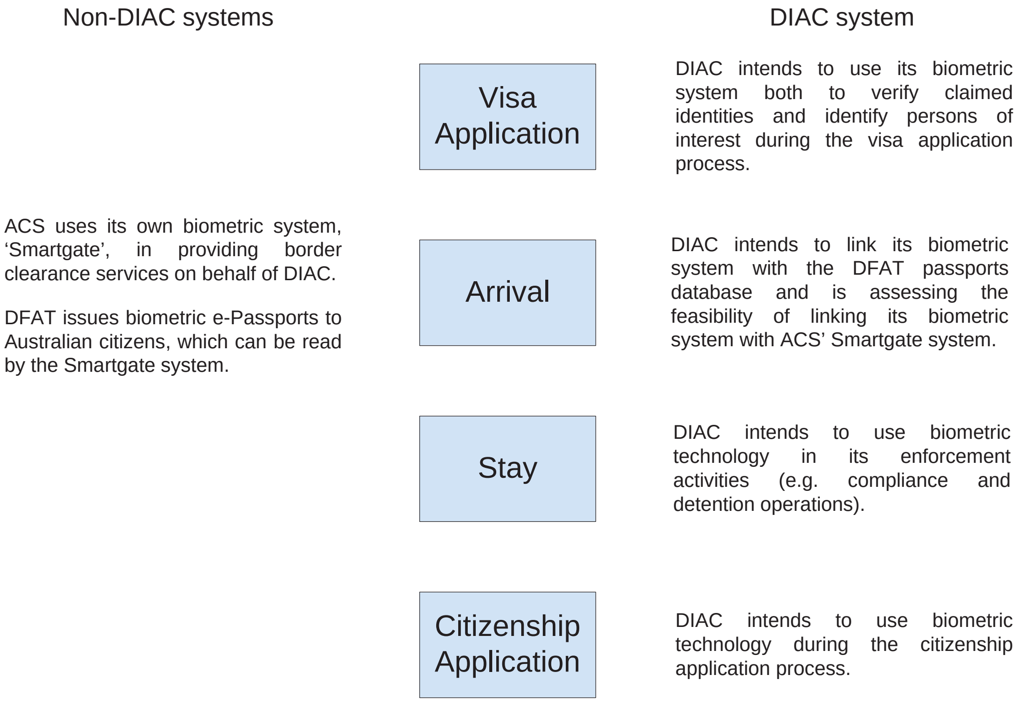
1.16 The biometric projects planned by DIAC potentially could encompass a series of decision points ranging from when a non-citizen first seeks to come to Australia, their arrival, their stay in the country, and sometimes their application for citizenship.[35] Figure 1.1 shows examples of DIAC's intended use of its biometric systems as they relate to the decision points, as well as the principal non-DIAC systems.

[34] The Biometrics for Border Control initiative started prior to the introduction of DIAC's Systems for People (SfP) initiative. As a result of certain recommendations of the Palmer report (see footnote 39), detention centres were given the highest priority for the introduction of biometrics (through SfP). The project that was initiated, Detention Centre Rollout (DCR), was funded from both the SfP/Palmer and the Biometrics for Border Control initiative.

[35] DIAC advised that it has also been enhancing their non-biometric identity checking through improvements in biographical data and checking of credentials.

Figure 1.1

Potential uses of biometric systems in the movement of people into and out of Australia



DIAC intends to use its biometric system both to verify claimed identities and identify persons of interest during the visa application process.

ACS uses its own biometric system, ‘Smartgate’, in providing border clearance services on behalf of DIAC.

DFAT issues biometric e-Passports to Australian citizens, which can be read by the Smartgate system.

DIAC intends to link its biometric system with the DFAT passports database and is assessing the feasibility of linking its biometric system with ACS’ Smartgate system.

DIAC intends to use biometric technology in its enforcement activities (e.g. compliance and detention operations).

DIAC intends to use biometric technology during the citizenship application process.

Source: ANAO

1.17 DIAC has identified the key benefits to the Australian Government and society derived from an increased focus on the verification of identity and the employment of biometric tools as:

- establishment of a ‘foundation identity’ for non-citizens to use in the Australian community, from initial contact through to when they become Australian citizens;
- enhanced national security through detection and referral of persons of concern during the visa application process;
- consolidation of client identity data in DIAC systems;
- facilitation of border movements and increased detection of identity fraud and any substitution at the border;
- ready identification of persons who breach visa conditions;
- greater protection for Australian residents from identity theft;

- greater protection for Australian industry and government from identity fraud; and
- greater confidence in the identity of the non-citizens who are future Australian citizens.[36]

Costs and benefits can be difficult to assess

1.18 Biometrics are intended to supplement or even replace manual identity checks and potentially can increase speed, consistency and accuracy of identity checking as well as potentially increasing confidence about a person's identity. Internationally, there is increasing focus on this technology as a tool in mitigating risks of identity fraud. The stated benefits of biometrics in the area of border security generally relate to reduced rates, and financial impacts, of identity fraud, improved confidence in administration and national security, and greater efficiency in border processing.[37]

1.19 The costs generally relate to expenses incurred in introducing and administrating the systems, as well as potential non-financial costs relating to privacy as it concerns the use and security of personal data held by government agencies.[38] Some of these costs and benefits are difficult to quantify. Also, the 'avoided cost' of failure to identify people accurately is difficult to estimate.

1.20 That said, the risks posed by identity crime, including fraud, are significant. For example, identity fraud costs the Australian community an estimated $1.1 billion per annum.[39] In addition, identity fraud committed against government agencies such as DIAC can have downstream financial costs. For example, government agencies are the sources of most Proof of Identity (POI) documents that are often used to commit identity fraud in the private sector.[40]

[36] DIAC, 2007, *Identity Matters: Strategic Plan for Identity Management in DIAC 2007–2010*, p. 31.

[37] See for example: The Hon. Alexander Downer MP, Minister for Foreign Affairs; Senator the Hon. Amanda Vanstone Minister for Immigration and Indigenous Affairs Multicultural and Indigenous Affairs; Senator the Hon. Christopher Ellison Minister for Justice And Customs Joint Media Release, 10 May 2005, *Development Of Biometric Technology For Border Control*.

[38] See for example: <http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html>, [accessed 11 September 2007].

[39] Securities Industry Research Centre, 2003, *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent.* The private sector generally bears the brunt of identity fraud in terms of frequency and cost – the cost of identity fraud to individual Australian Government agencies has not been estimated.

[40] Securities Industry Research Centre, 2003, *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent.*

1.21 For DIAC, there have also been several high-profile cases where the department was unable to identify people it has detained on suspicion of being unlawful non-citizens. These people were in fact lawfully in Australia, and the failure to identify them had 'catastrophic' results for these individuals and reputational consequences for DIAC.[41]

DIAC's business environment

1.22 Shortly after the announcement of the introduction of the *Biometrics for Border Control* initiative (May 2005), the Government announced substantial administrative and systems reform for DIAC in response to the Palmer and Comrie Reports.[42] Funding of $231 million over four years was announced in October 2005 for what became known as the 'Palmer Implementation Plan'.[43]

1.23 The Palmer Implementation Plan included substantial changes to DIAC's governance and client service arrangements and staff professional development.[44] As part of this Plan, DIAC commissioned a review of its information requirements and systems.

1.24 The results of DIAC's review of its information requirements and systems gave rise to the 'Systems for People' initiative announced in May 2006 ($495 million over four years).[45]

1.25 Both the Palmer Implementation Plan and Systems for People changes post-date DIAC's biometrics program, but have direct and indirect influences on the biometrics projects. [46]

1.26 Notwithstanding the substantial additional funding provided to the department, DIAC has found its overall budget position to be challenging.

[41] See for example: M J Palmer 2005 *Inquiry into the Circumstances of the Immigration Detention of Cornelia Rau*; Commonwealth Ombudsman 2005 *Inquiry into the Circumstances of the Vivian Alvarez Matter*; Commonwealth Ombudsman 2006 *Department of Immigration and Multicultural Affairs, Report on Referred Immigration Cases: Mr T*.

[42] MJ Palmer, op.cit*,* 2005*;* and Commonwealth Ombudsman, op. cit, 2005.

[43] DIMIA, September 2005, *Report from the Secretary to Senator the Hon Amanda Vanstone Minister for Immigration and Multicultural and Indigenous Affairs: Implementation of the Recommendations of the Palmer Report on the Inquiry into the Circumstances of the Immigration Detention of Cornelia Rau.* See also Amanda Vanstone, Minister for Immigration and Multicultural Affairs, 6 October 2005, *Palmer Implementation Plan and Comrie Report*.

[44] DIAC Secretary letter to the Auditor-General, 13 December 2006.

[45] Amanda Vanstone, Minister for Immigration and Multicultural Affairs media release, 9 May 2006, *Palmer and Comrie Reports Guide DIMA's Budget*.

[46] An example of a direct impact would be the substantial change in the systems environment in which biometrics were to be introduced. An indirect influence would be the changed governance arrangements. Future ANAO audit activity may assess the implementation of the DIAC change agenda.

Expenditure exceeded revenue by 1.7 per cent and 4.3 per cent in 2005–06 and 2006–07 respectively, with a smaller deficit (0.4 per cent) forecast for 2007–08.[47] The department took steps to reduce project and program area expenditure in 2006–07 and is seeking to make further cuts in 2007–08.

DIAC IT environment

1.27 DIAC's Systems Delivery and IT Services and Security Divisions service the department's IT needs. Several third parties are contracted to provide IT support services.[48]

1.28 In August 2004, DIAC concluded its assessment into biometric solution alternatives and sourcing strategies. Two solutions were proposed: [49]

- Biometric Services—the biometric technology; and
- Identity Services—the business rules and system integration logic.

1.29 A contractor was selected as DIAC's strategic biometrics partner to provide a suite of suitable biometric solutions, software tools and a range of identity management services, including research.[50] As a result, DIAC has selected a commercial off-the-shelf biometric software product.

1.30 At the time of the audit, two system development projects were underway, the Identity Services Repository (ISR) and the Detention Centre Rollout (DCR).[51]

Identity Services Repository (ISR) project

1.31 The ISR project, which commenced in mid-2004 and is ongoing, provides the basis for a consistent approach to the management of client identity information held by DIAC. It is a cornerstone of DIAC's Identity Management strategy and will support the Systems for People initiatives relating to DIAC client service. [52]

[47] See DIAC *2006–07 Portfolio Budget Statements*, p. 94 and DIAC *2007–08 Portfolio Budget Statements*, p. 93.

[48] DIAC's main IT service providers include: Unisys; Computer Sciences Corporation (CSC); and IBM.

[49] DIAC, 2004, *Identity Services Implementation Options Paper*.

[50] DIAC released a tender in November 2005 and selected the preferred supplier in September 2006.

[51] These followed on from the recommendations of the Identity Services Implementation Options Paper, which recommended that Identity Services be developed in-house to retain flexibility, and that the Biometric Services solution be procured (purchased or leased).

[52] DIAC, 2007, *Identity Services Repository Training Guide—Using the ISR*, Version 3.0.

1.32 It is envisaged that the ISR will:

- assist DIAC officers in establishing and verifying a client's identity; and
- become DIAC's repository for all information relating to the identity of DIAC clients. This includes biographic, documents, facial images and, potentially, other biometric information.

1.33 Currently,[53] the ISR connects to several DIAC business applications. Upon implementation of the biometric solution (see Detention Centre Rollout project below), the ISR will interface with the DIAC biometric system. Appendix 1 illustrates the current and proposed ISR system interfaces.

Detention Centre Rollout (DCR) project

1.34 The collection of personal identifiers[54] from detainees would assist DIAC with identity establishment and verification by enabling staff to conduct biometric searches against DIAC's Identity Service and databases held by other agencies.[55] Acquiring personal identifiers, such as a fingerprint, should enable DIAC to use this information to assess its confidence in the identity presented by a client.[56]

1.35 The objectives of the DCR project are to:

- introduce processes to acquire digital facial images and finger scan;[57]
- introduce the ability to store, retrieve and match biometric quality data from a national database;[58] and
- deliver the infrastructure, facilities, hardware, software and training to support the introduction of biometric systems in detention facilities. [59]

1.36 The same contractor is working in partnership with DIAC on the DCR project.[60] Figure 1.2 represents the architecture of the DCR project.

[53] As at completion of ISR Phase 6, June 2007.

[54] Personal identifiers includes biometrics.

[55] DIAC, 2006, *DCR Project Phase 1 – Requirements Specification*, Final Version: 1.0.

[56] In cases where the confidence level is low or where no identity has been presented by a client, this personal identifier can be compared with like data (where it exists) held by other agencies within Australia and overseas.

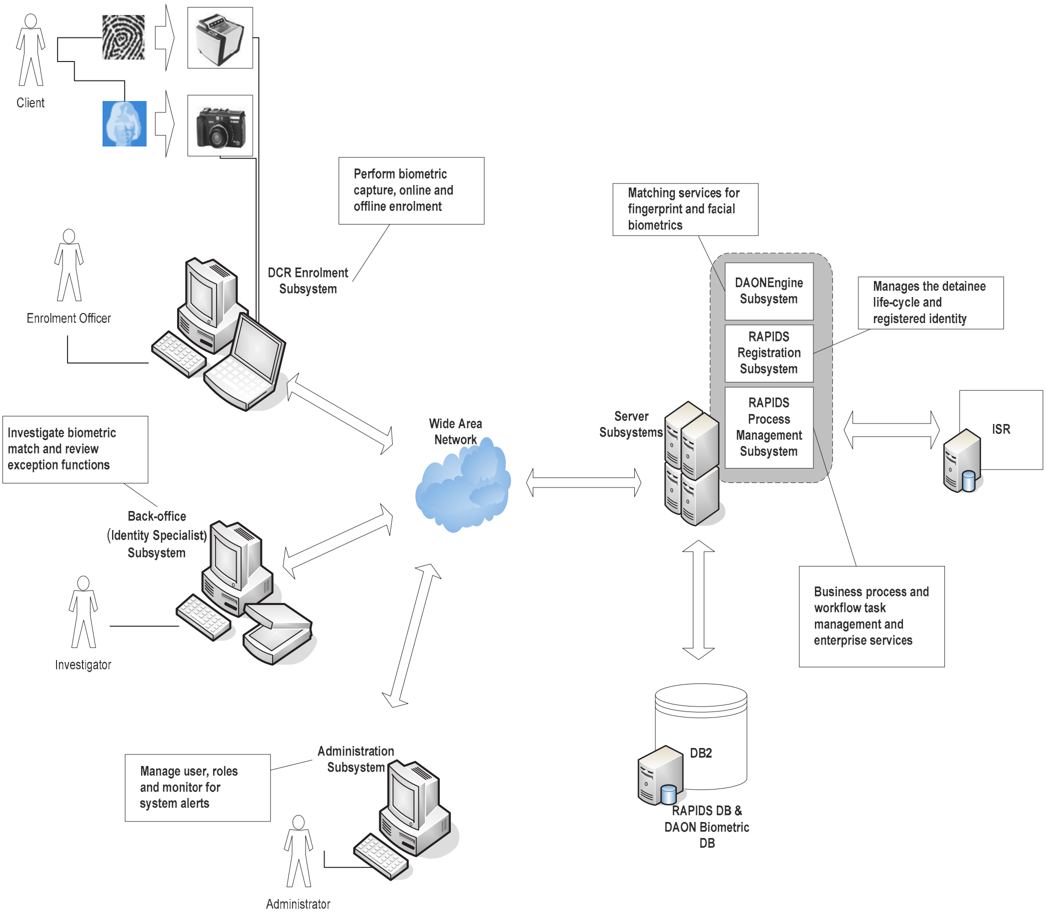
[57] A biometric enrolment process is to be introduced as the first step of the detention reception process. During biometric enrolment the detention services provider will use the biometric acquisition suite to acquire digital facial images and finger scans from detainees.

[58] The biometric acquisition suite and software will be integrated with the ISR enabling the national storage, retrieval, matching and referral of digital facial images and finger scans.

[59] DIAC, 2007, *Detention Centre Rollout of Biometrics—IT Project Management Plan*, Version: 2.0.

Figure 1.2

Proposed DCR Project Biometric Solution Architecture—July 2007


Client
Perform biometric capture, online and offline enrolment
DCR Enrolment Subsystem
Enrolment Officer
Matching services for fingerprint and facial biometrics
DAONEngine Subsystem
RAPIDS Registration Subsystem
RAPIDS Process Management Subsystem
Manages the detainee life-cycle and registered identity
ISR
Investigate biometric match and review exception functions
Wide Area Network
Server Subsystems
Back-office (Identity Specialist) Subsystem
Investigator
Business process and workflow task management and enterprise services
Manage user, roles and monitor for system alerts
Administration Subsystem
DB2
RAPIDS DB & DAON Biometric DB
Administrator

Source: ANAO based on DIAC documentation.

1.37 Appendix 2 shows the client-side and server-side subsystems of the proposed biometric solution.

The audit

Objective and scope

1.38 The objective of the audit is to determine whether DIAC's biometrics program had appropriate:

[60] The DCR project has three stages. Stage one was completed in November 2006; stage two is currently in progress, and stage three is scheduled for completion by January 2008.

- business review processes (including a business case);
- authorisation;
- business and IT governance arrangements; and
- IT project management and systems development arrangements.

1.39 The audit scope was on the design and planning for the introduction of biometrics in DIAC. Matters concerning the implementation of the technology in DIAC and arrangements with other agencies in relation to the '*Biometrics for Border Control*' initiative were outside the audit scope.

Method

1.40 The audit method comprised:

- development of audit criteria with assistance from an expert advisor and in consultation with DIAC;
- interviews with DIAC managers and staff;
- use of specialist ANAO IT auditors;
- consultation with the OPC and CrimTrac; and
- analysis of DIAC documentation and data.

1.41 The audit was conducted in conformance with ANAO auditing standards at a cost to the ANAO of $425 000.

Audit report

1.42 The report is structured into the following four chapters:

- Chapter 1—Background and Context: provides background and context to DIAC's introduction of biometrics and sets out the audit objective and scope, audit method and structure of the report;
- Chapter 2—Planning for Implementation: examines DIAC's business case, benefits and costs, DIAC's initial planning, authority for the introduction of biometrics and the requirement for full interoperability of its biometric technology with other countries;
- Chapter 3—Governance Arrangements: examines DIAC's business governance, IT governance, IT project management, and project funding arrangements; and

- Chapter 4—Administrative Arrangements: assesses DIAC's guidance and training, mechanisms for assuring privacy, and its IT system development.

2. Planning for Implementation

This chapter examines DIAC's planning for the introduction of biometrics.

Introduction

2.1 Effective planning for implementation is a critical factor to an agency's ability to prepare successfully for intended policy outcomes.

2.2 To assess DIAC's planning for implementation, the ANAO examined:

- DIAC's initial research, business case, benefits and costs for the introduction of biometrics;
- DIAC's initial planning;
- the authority for the introduction of biometrics in DIAC; and
- the requirement for full interoperability of DIAC's biometric technology with other countries.

Initial research

2.3 From the late 1990s to 2003, Australian border security agencies had been considering the potential benefits of biometrics following international developments and increasing focus on this technology (see paragraphs 1.10 to 1.14).

2.4 In January 2003 DIAC prepared a report that examined the specific nature and management of issues and risks related to immigration and citizenship identity fraud.[61] The report found no evidence to suggest widespread identity fraud problems, however, there were anecdotal examples of immigration and identity fraud that were said to be complex, varied in nature and difficult to investigate and dismantle.[62]

2.5 The same report prompted further research into biometrics. A number of tests and trials were conducted to determine the biometric types and technologies that would align with DIAC's business needs and requirements.

[61] DIMIA, 2003, *The Prevention and Management of Identity Fraud against DIMIA Programs*.

[62] Ibid. Examples of immigration and identity fraud include: allegations concerning certain nationals who have provided false identities and had been granted Temporary Protection Visas; and nationals who use the Protection Visa system to gain employment rights in Australia.

Tests and trials

2.6 In October 2003, DIAC began collecting business requirements from across the department and its major stakeholders to assess whether biometrics capability could assist in identity and fraud management.[63]

2.7 In May 2004 the Government announced that DIAC had been given funds for twelve months to undertake research and test the best way to incorporate biometric technologies into Australia's existing advanced electronic visa and entry arrangements.[64]

2.8 DIAC conducted several tests and trials of biometric technologies. The core tests and trials assessed by the ANAO include: the Biometrics Discovery Project; the Biometrics Test Facility Project; and the Biometrics Trials Overseas. The Defence Science and Technology Organisation (DSTO) conducted various analyses into the effects associated with biometric enrolment and verification on DIAC. Appendix 3 lists the reports produced by the DSTO on these analyses.

2.9 The tests, trials and the resulting reports from both the DSTO and DIAC, provided valuable information and guidance to the department in determining the way to move forward with biometrics.

Business case

2.10 To confirm that the business case is robust, it should meet the business need and demonstrate that the program or project is affordable, achievable and represents value for money.[65]

2.11 A business case also examines a wide range of options that will meet the business need. The range of options considered should include maintaining the status quo. A rigorous assessment of the pros and cons is conducted of each option to determine its potential to meet the critical success factors.[66]

2.12 The ANAO reviewed DIAC's business case, prepared in early 2005, for a phased application of biometrics. The ANAO found that DIAC identified sound reasons why the business case should be approved. It also assessed in a

[63] Known as the 'Biometrics Requirements Discovery Project'.

[64] Media release 11 May 2004.

[65] Department of Finance and Administration, *Gateway Review Process – A Handbook for Conducting Gateway Reviews,* August 2006, Canberra, p. 28.

[66] ibid. Options are also appraised in accordance with principles which are relevant and appropriate for responding to the business need.

high-level manner the consequences of: no additional funding; minimum funding; and full funding for biometrics at the border. However, the business case did not refer to non-biometric options for improving DIAC's client identity management, although work on non-biometric components of identity management (such as legislative changes, improvements to business processes and a document verification system) is evident in a range of other DIAC documents. In addition, there were no figures (precise or estimates) of how much identity fraud was actually affecting the department.

2.13 DIAC documentation shows that there was internal (from the DIAC Executive) and external (from other Australian Government agencies) support for the project.[67]

2.14 The ANAO found that the scope and requirements were apparent in the business case. However, the business case did not include a clear timeframe for the project development, except stating that it was to be a phased approach.

2.15 DIAC identified major risks and developed a risk management plan eventually. DIAC also established high level critical success factors, which were made more specific in subsequent plans.

Benefits and costs

2.16 Project evaluations should assess, inter alia, the extent to which the intended benefits have been achieved.

2.17 In early 2005, DIAC prepared a cost-benefit analysis as part of the *Biometrics for Border Control* initiative.[68] However, this document was very high-level and contained little in the way of analysis. Neither this document, nor subsequent analysis have ever determined the size of the 'problem' being addressed through the introduction of biometric technologies in DIAC. The estimated cost was $42.87 million over four years.

[67] The business case also included a management or program outline.

[68] The benefits from the initiative were expressed in very general terms, such as 'greater certainty', 'increases our ability', 'reduces opportunities', without stating what the original level was nor the extent to which it would change under the initiative.

2.18 Later in 2005,[69] the key benefits to government from DIAC's introduction of biometrics were identified as:

(1) improved national security through more effective identity screening mechanisms offshore. The biometric alert list matching process will identify persons of concern before travel to Australia allowing the risk to be managed offshore;

(2) reduced identity fraud due to better identity management of non-citizens in Australia;

(3) assistance in the removal of unsuccessful asylum seekers in detention; and

(4) reduced capacity for the use of fraudulent identities by protection visa applicants and the consequent reduction in costs to the legal system from this litigious group.

2.19 A benefits realisation plan is useful in clearly tracking what will happen across a program, where and when the benefits will occur and who will be responsible for the delivery.[70] The ANAO found that there was no benefits realisation plan, although some of the individual projects did include a benefits realisation component as part of their project plans.

2.20 The ANAO considers that the expected benefits identified by DIAC (see paragraph 2.18 above) are assessable, however, to be meaningful, the department would require a means for monitoring changes over time that could account for exogenous influences on these changes. At the time of the audit, DIAC did not have a suitable monitoring mechanism, nor a strategy to allow the effectiveness of its chosen biometric solution in delivering its expected benefits to be evaluated.

2.21 However, the ANAO noted that the DIAC program area had recently established an evaluation and monitoring team, with a view to establishing performance measures and baseline data.[71] The ANAO considers that this is a

[69] At the time, DIAC expected that the successful deployment of biometrics would be reflected in: more referrals and turnarounds at Australia's port of entry; increased border security through the matching against biometric alert lists; more seamless processing of legitimate travellers; and increased detection of fraudulent use of identity in travel to Australia and access to benefits or entitlements.

[70] See: <http://www.ogc.gov.uk/documentation_and_templates_benefits_realisation_plan_.asp>, [accessed 3 December 2007].

[71] Baseline data could include initial quantitative or qualitative information built-up over one year, to be used later as a benchmark from which deviations and/or changes may be assessed to make informed decisions in the future.

useful first step in developing an effective monitoring and evaluation capability.

2.22 Overall, the ANAO considers that DIAC's business case for the introduction of biometrics was generally sound. Reasons were identified why the business case should be approved, and the expected benefits and costs are assessable. However, for the assessment to be meaningful, DIAC would benefit from a more structured approach to monitoring changes arising from its introduction of biometrics over time and evaluating the effectiveness of its chosen biometric solution. This is necessary to support management decisions about future directions in this area.

Planning for biometrics

Overarching plans

2.23 Experience indicates that the likelihood of effective cross-agency implementation is greater when there is an overarching, high-level implementation plan that is coordinated by a nominated lead agency and has clearly defined critical cross-agency dependencies and responsibilities.[72]

2.24 A number of planning documents have been prepared for the introduction of biometrics. The key documents are outlined below.

Implementation Plan of the 'four-agency initiative'

2.25 A cross-agency working group prepared the Implementation Plan of the 'four-agency initiative',[73] *Biometrics for Border Control Implementation Plan 2005—2009*.[74] The Department of Foreign Affairs and Trade (DFAT) was the lead coordinating agency of this initiative for 2006–07 and towards the end of 2006, DIAC took over the role.[75]

[72] ANAO *Better Practice Guide-Implementation of Programme and Policy Initiatives Making Implementation matter,* October 2006*,* Canberra, p. 26.

[73] The four agencies comprise: the Department of Foreign Affairs and Trade (DFAT), Australian Customs Service (ACS), the Department of Immigration and Citizenship (DIAC), and the Office of the Privacy Commissioner (OPC).

[74] The *Biometrics for Border Control Implementation Plan 2005—2009* includes information (i.e. phased implementation strategy; success criteria; benefits statement; work breakdown structure; funding; risk management etc.) aimed to assist the four agencies: DFAT; ACS; DIAC and the OPC, who are involved in the four-year development of biometrics for border control.

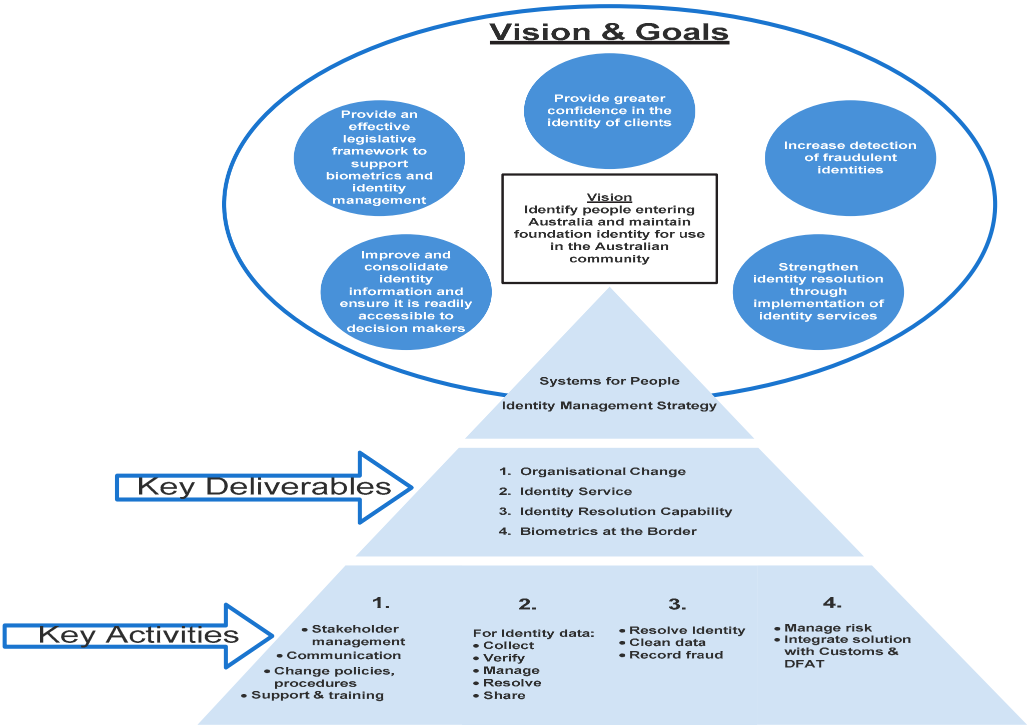
[75] DIAC volunteered to be the lead coordinating agency, and the inter-departmental working group accepted this arrangement. The *Biometrics for Border Control Implementation Plan 2005–2009* states that 'a Working Group consisting of DFAT, Customs, and DIAC monitors cross-agency matters with the assistance of the Inter-Departmental Committee (IDC). It is to achieve this by meeting on a regular basis'.

DIAC Strategic Plan

2.26 In February 2007, DIAC finalised its strategic plan for identity management.[76] This plan represented a statement of the vision for the management of client identity as an integrated DIAC business function.[77] Figure 2.1 shows DIAC's identity management strategy.

Figure 2.1

DIAC's Identity Management Strategy


Vision & Goals
Provide greater confidence in the identity of clients
Provide an effective legislative framework to support biometrics and identity management
Increase detection of fraudulent identities
Vision
Identify people entering Australia and maintain foundation identity for use in the Australian community
Improve and consolidate identity information and ensure it is readily accessible to decision makers
Strengthen identity resolution through implementation of identity services
Systems for People
Identity Management Strategy
Key Deliverables
1. Organisational Change
2. Identity Service
3. Identity Resolution Capability
4. Biometrics at the Border
Key Activities
1.
• Stakeholder management
• Communication
• Change policies, procedures
• Support & training
2.
For Identity data:
• Collect
• Verify
• Manage
• Resolve
• Share
3.
• Resolve Identity
• Clean data
• Record fraud
4.
• Manage risk
• Integrate solution with Customs & DFAT

Source: DIAC.

2.27 The Strategic Plan is focused on the implementation of identity management as part of the Systems for People (SfP) business transformation process.[78] The plan includes an extensive roadmap of what needs to be done to achieve the expected outcomes for the years 2007–2010.

[76] DIAC's strategic plan is called, *Identity Matters: Strategic Plan for Identity Management in DIAC 2007–2010.* This document was released within the agency in May 2007, and published on the department's website in September 2007.

[77] DIAC, *Identity Matters – Strategic Plan for Identity Management in DIAC 2007–2010,* May 2007, p. 4.

[78] DIAC, *Identity Matters – Strategic Plan for Identity Management in DIAC 2007-2010,* May 2007, p. 4.

DIAC Implementation plan

2.28 In August 2007, DIAC finalised an internal Implementation Plan for identity management for 2007–08.[79] This Implementation Plan aims to support DIAC's strategic plan by translating the key deliverables into practical tasks for the effective development and delivery of enhanced identity management.[80]

Timelines for critical steps

2.29 The *Biometrics for Border Control Implementation Plan 2005—2009* includes a milestone map that illustrates the high-level implementation strategy.[81] DIAC's *Identity Matters: Strategic Plan for Identity Management in DIAC 2007–2010* addresses the roadmap for both business and IT deliverables.

2.30 Appendix 4 illustrates the timeline for expected deliverables for the period January 2007 to June 2009.

2.31 The ANAO considers the Implementation Plan of the 'four-agency initiative', DIAC's Implementation Plan, and its Strategic Plan as useful initial documentation for the planning of biometrics. They are extensive, thorough, and adhere to sound practice. DIAC established clear timelines that set adequate review points for both business and IT deliverables. DIAC's adherence to these timeframes is discussed below.

Are timelines being met?

2.32 The ANAO analysed the milestones set out in the various plans, particularly DIAC's Strategic Plan, focusing on the timeframes set to deliver both business and IT deliverables.

2.33 The ANAO found that there have been delays in the delivery of specific capabilities. For example, at the time of the audit, the collection and matching of finger scans and digital facial images (to the required legal and technical standard) for detention processing has been postponed. This capability was expected to have been delivered on 30 June 2007.[82]

[79] DIAC's implementation plan is called *Making the Identity Management Strategy a Reality*.

[80] DIAC, *Implementation Plan 2007–2008, Identity Management in DIAC – Making the Identity Management Strategy a Reality,* 20 August 2007, p. 5. In addition, DIAC's Implementation Plan details the following: the full range of activities in DIAC's Identity Branch's plan for 2007–08; the alignment of the various tasks to the strategic goals and objectives to which they contribute; the groups within Identity Branch what will carry out the work; and a link to the tasking sheets for the key tactics and activities.

[81] The high-level implementation strategy mainly relates to business deliverables.

[82] DIAC, *Identity Matters – Strategic Plan for Identity Management in DIAC 2007–2010,* May 2007, p. 39. Similarly, interfaces with Crimtrac for sharing and checking finger scans should have occurred on 30 June 2007, this has now moved to November 2007.

Success factors and critical dependencies

2.34 Implementation plans should spell out critical intermediate and final milestones and results, and identify areas of risk, and how and when they will be clarified and/or treated.[83] These should be identified at the early stages to draw together all the dependencies to the factors that affect success in a program, such as the delivery of other projects. The ANAO assessed whether the various strategic and implementation plans appropriately addressed these issues.

2.35 All the planning documents for the introduction of biometrics in DIAC clearly stipulated success factors. For example, both the Implementation Plan of the 'four-agency initiative' and DIAC's Implementation Plan included critical success factors and performance measures that aligned with its outputs and activities.

2.36 Further, DIAC's Strategic Plan for Identity Management stated critical success factors, mainly dependencies that would affect not only the introduction of biometrics, but also the successful implementation of identity management as a whole. For example, the most significant dependency identified for the development of biometrics at DIAC was the availability of the SfP technical resources to support identity management projects.[84]

2.37 Overall, the ANAO considers that DIAC had sound initial planning for the key elements for the introduction of biometrics. Several tests and trials were conducted, and its planning documents (both implementation and strategic plans) established clear timelines, adequate review points, and unambiguous success factors including critical dependencies.

Authority

2.38 The introduction of new technologies such as biometrics, requires authority, where appropriate.[85] This provides a basis for a set of business rules

[83] ANAO *Better Practice Guide-Implementation of Programme and Policy Initiatives Making implementation Matter,* October 2006, Canberra, p. 26.

[84] See: DIAC, *Implementation Plan 2007–2008; Identity Matters–Strategic Plan for Identity Management in DIAC 2007–2010*, pp. 36–37; and *Identity Management in DIAC-Making the Identity Management Strategy a Reality,* 20 August 2007, p. 10). SfP is a technology enabled transformation of the way DIAC does business. Delays in SfP projects will ultimately affect delivery of biometric capabilities. From 30 June 2007, the Identity Branch's newly created Projects Portfolio Group is responsible, inter alia, for the integration of identity projects with SfP releases through an assigned SfP program manager. The ANAO considers that this function should enhance DIAC's focus on the integration of the biometric projects with SfP deliverables.

[85] Authority such as legislation and/or government decision.

and procedural guidelines within which the technologies can operate, and helps ensure that there is a basis for correct, consistent and equitable decision making that accords with the law and government policy.

2.39 The ANAO examined the authority and procedural guidelines developed in preparation for DIAC's introduction of biometrics.

Government mandate for DIAC to introduce biometrics

2.40 Government has authorised activity in relation to the introduction of biometrics on several occasions.

2.41 In October 1999 the Government authorised that amendments be prepared to the M*igration Act 1958* to strengthen and clarify powers to identify unauthorised arrivals and asylum seekers, using fingerprinting and other means of biometric testing. Authority to use these powers was to be sought once the legislation was in place. As discussed below, legislative amendments were passed into law in 2004.

2.42 In 2004, the Government authorised DIAC to research and test:

> the best way to incorporate biometric technologies into Australia's existing advanced electronic visa and entry arrangements … [and to] develop a capacity to store and use digital biometric images to better identify its clients each time they deal with the Department.[86]

2.43 This funding, which was for twelve months, was followed by government authorisation of the four-year initiative, known as *Biometrics for Border Control* in 2005. As part of the initiative DIAC was authorised to:

> implement biometric technology for border security and identity verification. This technology will enable better identification and screening of non-citizens seeking to enter Australia.[87]

2.44 The interdependent projects approved by the Government were:

a) Evaluation, procurement and deployment of biometric equipment for static and mobile use;

b) Full integration of the new identity services repository (ISR) with existing DIAC systems;

c) Implementation of biometric matching, verification and identification;

[86] Amanda Vanstone, Media release 11 May 2004.

[87] Amanda Vanstone, Media Release, 10 May 2005.

d) The collection of images across all DIAC business processes (including through e-visa processes and third party enrolments) using a universal biometric enrolment portal;

e) The biometric matching of all images collected against national security alerts in MAL which have images attached;

f) Linking the ISR with the Australian and New Zealand passport database; and

g) Assessing the feasibility of linking biometric information in DIAC and Customs border systems.

2.45 In May 2006, the Government authorised substantial systems changes in DIAC, known as Systems for People (SfP). SfP included a new biometric project, rolling-out of biometrics to compliance areas as well as detention centres. Funding for one of the *Biometrics for Border Control* projects, the Identity Services Repository, was moved into the SfP projects.

Legislative authority

2.46 The Minister for Immigration and Citizenship administers Australia's immigration and citizenship legislation. Collectively, the legislation[88] set out the legal framework for how non citizens can enter, stay in, and leave Australia, and how they can join the Australian body politic. [89]

Migration and citizenship legislation has been amended to address the collection, use, access/disclosure and retention/destruction of personal identifiers

2.47 In October 1999 the Government authorised amendments to the M*igration Act 1958* to strengthen and clarify powers to identify unauthorised arrivals and asylum seekers, using fingerprinting and other means of biometric testing.[90] This legislation was to complement powers to prevent 'forum

[88] The *Migration Act 1958*, the various citizenship Acts, and supporting Regulations.

[89] Commonwealth of Australia, *Administrative Arrangements Order*, 21 September 2006, as amended 30 January 2007 lists the *Migration Act 1958* and the *Australian Citizenship Act 1948* as legislation administered by the Minister. Subsequently, the *Australian Citizenship Act 1948* has been repealed (by the *Australian Citizenship (Transitionals and Consequentials) Act 2007*) and replaced by the *Australian Citizenship Act 2007*. The Minister also administers the *Australian Citizenship Act 1973*. The Administrative Arrangements Order is yet to be updated to reflect the new legislative framework.

[90] Including DNA testing, face, palm or retinal recognition, and voice testing.

shopping'[91] and issue unauthorised arrivals with temporary protection visas in the first instance.[92]

2.48 Following consideration by parliament, including committee review,[93] the *Migration Legislation Amendment (Identification and Authentication Act 2004* was passed into law. The Act addresses the collection, use, access/disclosure and retention/destruction of *personal identifiers*:

(a) fingerprints or handprints of a person; [94]

(b) a measurement of a person's height and weight;

(c) a photograph or other image of a person's face and shoulders;

(d) an audio or a video recording of a person; [95]

(e) an iris scan;

(f) a person's signature; and

(g) any other identifier prescribed by the regulation.[96]

2.49 Biometric technologies enable personal identifiers to be measured, such as by use of a computer-generated template or algorithm. Appendix 5 lists the stated purposes of personal identifiers.

Migration and citizenship legislation's approaches to establishing identity

2.50 The *Migration Act 1958*, as amended, enables personal identifiers to be collected and used by decisions makers at various decision points.

2.51 There is no specific requirement under the *Migration Act 1958* for the Minister or his/her delegates to be satisfied that a person is who they claim to be. Instead, the Act provides a framework for identity checking at various

[91] Forum shopping occurs when a person ignores or abandons protection already available to them and chooses to use their ability to claim refugee status to obtain a migration outcome in a country of their own preference (see DIMIA, *Annual Report 2001–02).*

[92] The scope of the proposed legislative amendments was progressively revised. By 2001, the persons who could be required to provide a biometric identifier had been broadened to, potentially, all non-citizens. By 2004, the final legislation excluded the collection of DNA samples.

[93] Senate Legal and Constitutional Legislation Committee, September 2003, *Provisions of the Migration Legislation Amendment (Identification and Authentication) Bill 2003.*

[94] Including those taken using paper and ink or digital livescanning technologies.

[95] Other than a video recording under section 261AJ.

[96] Other than an identifier the obtaining of which would involve the carrying out of an intimate forensic procedure within the meaning of section 23WA of the *Crimes Act 1914.*

decision points.[97] The Act also sets out administrative rules for the collection, retention and destruction of personal identifiers.

2.52 Australia's citizenship legislation was revised after the amendments to the *Migration Act 1958*. The *Australian Citizenship Act 2007* replaced the 1948 Act.[98] Unlike the *Migration Act 1958*, the *Australian Citizenship Act 2007* contains provisions that, where people seek to acquire citizenship by application, the Minister must be satisfied of their identity.[99] The new Act also addresses the collection, use, access/disclosure and retention/destruction of people's personal identifying information.

Consistency between policy intentions and legislation

2.53 Under the *Migration Act 1958*, a personal identifier is taken not to have been provided if it is unusable, of poor quality, or if the authorised officer is not satisfied about the procedure followed to obtain the personal identifier.[100] Furthermore, the Act states that a personal identifier is taken not to have been provided if an authorised officer is not satisfied about the integrity of the personal identifier that is provided.[101]

2.54 The ANAO found that the legislation does not define 'integrity', nor has DIAC obtained any specific legal advice on its meaning. The ANAO could find no explanation for DIAC's intent in its drafting instructions for the legislation.

2.55 DIAC's policy guidance indicates that 'integrity' is intended to mean that the officer 'has reasonable grounds to believe the identifier belongs to someone else.' Draft policy guidance gives five further examples of this (see paragraphs 4.3 to 4.5).

2.56 The ANAO found that the wording of the legislation expects DIAC decision makers to form judgements about the qualities of personal identifiers

[97] Decision points, including: visa application, visa decision, at the border (immigration clearance), cancellation and detention.

[98] The *Australian Citizenship Act 2007,* which includes provisions relating to personal identifiers, was prepared drawing on the experience gained in amending the more complex *Migration Act 1958.*

[99] *Australian Citizenship Act 2007*, sections 17(3), 19D(4), (24(3), and 30(3). The Minister may also be required to refuse the application on national security grounds.

[100] *Migration Act 1958*, Sections 5B (a), (c), (b)(ii).

[101] *Migration Act 1958*, Sections 5B (b)(i).

provided by DIAC clients.[102] However, DIAC's policy guidance indicates that the intention was not that the qualities of personal identifiers themselves should be assessed, but rather that assessment should be of the *claims* being made by people about the identifiers (that the personal identifiers are theirs). Consequently, there is a risk that the legislative wording is inconsistent with the policy intent which may have an adverse impact in the future. Consistency between the legislative wording and policy intent mitigates potential risks in an area that is contestable.

2.57 The ANAO notes that in passing the legislation, parliament required that the legislation be reviewed after three years of operation. The ANAO considers that the scheduled review (during 2008) of the legislation provides an opportunity for DIAC to review the consistency between legislative wording and policy intent.

Differentiating between 'requirements' and 'requests' for personal identifiers under the *Migration Act 1958*

2.58 Under the *Migration Act 1958* DIAC is authorised formally to require people to provide personal identifiers at various decision points, for example, whilst processing visa applications[103] and at immigration clearance.[104] These are discretionary powers, and DIAC staff may also request such identifiers more informally.[105]

[102] DIAC advised that unless a term is defined in legislation the meaning is taken from the Macquarie Dictionary. Using this approach, the ANAO considers that the legislation, as written, expects DIAC decision makers to form judgements about the specific qualities of the personal identifiers (such as the identifiers' moral qualities, wholeness or perfection).

[103] See *Migration Act 1958*, Sections 40(3) and 46 2(A).

[104] See *Migration Act 1958*, Section 166.

[105] DIAC advised the ANAO that clients do not have to provide personal identifiers unless they are formally required, notwithstanding that a form may instruct them to provide them or they may have been 'requested' to do so.

2.59 Whether the formal power to require the provision of personal identifiers has been invoked, or not, has consequential effects for decision makers. It is only when personal identifiers have been formally required that the decision maker is directly empowered to make decisions on the basis of the client's response. For example:

- s46(2(a)) of the Act renders an application invalid when personal identifiers have been formally required and these data fail to meet requirements set out in the Act;[106] similarly
- s40(3) of the Act, which deals with the circumstances in which a visa may be granted, authorises immigration officers formally to require visa applicants to 'provide one or more personal identifiers in relation to the application for the visa'. A visa application could be refused, under s65, when personal identifiers have been formally required and they fail to meet the requirements of the Act.[107]

2.60 DIAC has prepared standard letters for officers to use when formally requiring personal identifiers and when requesting personal identifiers. The letters formally requiring personal identifiers under s40 and s46 clearly state the consequences of failure to provide a personal identifier.

2.61 The distinction between 'requiring' and 'requesting' personal identifiers is subtle, but significant. There is a clear risk that clients may regard a 'request' from a DIAC officer as akin to a 'requirement'. The standard letter requesting personal identifiers includes advice 'if you do not do so before that date your application may be decided without this information being considered'. Neither the standard letters nor DIAC's information leaflet[108] adequately address this distinction to enable clients to understand fully the options open to them and the consequences of their choices. The ANAO considers that, consistent with its response to recommendations made by the Commonwealth Ombudsman,[109] DIAC should test and review its standard

[106] See also s5B.

[107] See also s5B.

[108] Form 1243i *Your personal identifying information.*

[109] During the audit, the Ombudsman published a report dealing with DIAC's obligation to provide an unsuccessful visa applicant with a letter that clearly explains the decision. The Ombudsman recommended that DIAC conduct a comprehensive review of its management of notification letters, including, inter alia, their quality and consistency. Specific recommendations in the report were for DIAC to introduce quality assurance measures, introduce consistent letter templates, use plain English in letters, improve the description of review rights and adopt minimum standards for explaining the reasons for decisions. DIAC accepted all the Ombudsman's recommendations. See: Commonwealth Ombudsman 2007 *Department of Immigration and Citizenship: Notification of Decisions and Review Rights for Unsuccessful Visa Applications*.

letters and information leaflet to ensure that clients are informed adequately about the differing legal consequences arising from departmental officers' 'requiring' or 'requesting' the provision of personal identifiers.

Full interoperability of biometric technology with other countries

2.62 DIAC has legislative authority to collect and use a broad range of biometric data, but has chosen to use the facial image as its primary biometric and has invested its resources accordingly. The focus on facial images as primary biometrics was consistent with the ICAO standard for e-passports, work already underway in DFAT and ACS, and DIAC's biometric discovery work which identified a business need for staff to be able to view digital photographs as part of application processing.

2.63 The ANAO found that there was nothing in the Government decision mandating the choice of a 'primary' biometric or use of any particular biometric.[110] In approving the *Biometrics for Border Control* initiative, the Government also decided that the four agencies give priority to ensuring that biometric technology was fully interoperable with similar technology developed by other countries.[111]

2.64 There are clear benefits in ensuring that DIAC's biometrics systems are interoperable with the systems being implemented in other agencies,[112] and overseas counterparts. The ANAO considers that, to the extent that these agencies use, or plan to use, facial biometrics,[113] DIAC can be said to be implementing the Government's requirement. However, the ANAO observes that DIAC's progress in linking its facial biometric system to the other agencies has been slow (see paragraph 2.70).[114]

[110] The government's focus was on Australia benefiting from the potential inherent in biometrics rather than on any one biometric solution.

[111] A framework for Australian Government information interoperability has also subsequently been issued by the Australian Government Information Management Office in 2006 called the *Australian Government Information Interoperability Framework*.

[112] Particularly ACS and DFAT.

[113] Often as part of a suite of biometrics.

[114] Future audit work may include the arrangements to exchange and manage information with partner agencies.

DIAC's choice of primary biometric limits its ability to use other biometric data for matching purposes

2.65 As discussed previously, there are two main uses for biometrics: identifying people, requiring 'one-to-many' matching; and verifying claimed identity, which requires 'one-to-one' matching. The ANAO notes that there is evidence that facial matching technology is much more effective at the latter than the former.[115]

2.66 Moreover, one-to-many matching requires comparison with data from persons of interest. In the case of data from overseas counterpart agencies and domestic criminal intelligence agencies, these data may more often be in the form of fingerprints rather than biometric quality photographs.

2.67 DIAC's main counterpart overseas agencies (USA and UK) are implementing multi-modal biometric systems, involving faces and fingerprints. This presents the possibility of one-to-many checking against their very large data holdings, particularly fingerprints.

2.68 Consequently, DIAC's focus on investing in facial matching capability means that it presently has limited capability to use other biometric data such as fingerprints for matching purposes, particularly for watch-list functions.

2.69 DIAC is aware of these limitations and has built its ISR with the capacity to store multiple biometrics.[116] The department has been working to develop some fingerprint capability, as it envisages the growth in the capture of fingerprint images across appropriate caseloads. [117] DIAC is also exploring linkages with Australian and overseas agencies in terms of accessing biometric data collected by them (see example below).

[115] The number of facial images in the database has a significant impact on identification accuracy (one-to-many). The more images to be matched against, the higher match error rate. Differences in the environments where the sample and enrolment images are taken effect both identification and verification (one-to-one) accuracy rates. For example, large-scale testing of facial matching technology has shown that images taken in exactly the same environment is likely to yield much better results than a stored image compared with live images. See: Bundeskriminalamt, *Gesichtserkennung als Fahndungshilfsmittel Foto-Fahndung*, February 2007 and DIAC, *Biometrics Discovery Project, Biometrics Steering Committee Report-Biometrics Performance and Cost Implications,* 15 January 2004.

[116] DIAC, 2007, *Identity Matters: Strategic Plan for Identity Management in DIAC 2007–2010*, p. 16. DIAC's detention centre roll-out project should also enable matching of detainee fingerprints with police databases.

[117] DIAC has two full-time fingerprint experts who are working to assist in the development of this capability.

Example: Working with CrimTrac

CrimTrac was established in July 2000 as an Executive Agency under the Commonwealth Public Service Act in the Attorney-General's portfolio in order to assist Australian police services to take advantage of opportunities opened up by forensic science, information technology and communications advances.[118] CrimTrac operates four systems to improve information sharing for police:

- a new National Automated Fingerprint Identification System (NAFIS);
- a National Criminal Investigation DNA Database;
- a National Child Sex Offender System; and
- the provision of rapid access to national operational policing data.

DIAC's documents indicate that the department was aware that there were potential efficiency and expertise gains from working with the CrimTrac system: establishing a separate database in the department would be 'very expensive; and wastes resources that could be spent elsewhere' and the department had 'no expertise'. Throughout 2001 and 2002, DIAC consulted with CrimTrac and the Attorney General's department and prepared a project proposal and purchasing plan and information brief. However, by October 2002, DIAC advised CrimTrac that, following amendments to its original legislative proposal, the department was 'considering the appropriate biometric data management strategies to support those amendments and further investigating the changes to departmental business requirements.' DIAC subsequently decided to build a separate biometrics system.

Since 2006, DIAC has been working with CrimTrac and the Australian Fisheries Management Authority in a project involving the use of 'livescan' fingerprinting technology to identify recidivist illegal foreign fishers in the Torres Strait. The ANAO considers that this approach demonstrates the value and ongoing potential for supplementing DIAC core facial matching systems with other technologies, where appropriate.

2.70 DIAC's early strategies have mainly focused on the use of face as a one-to-one matching capability. The current relatively limited fingerprint matching capability leaves the department in a position where it is unable to benefit fully from the international developments tending towards a broader use of fingerprints. To maximise the potential arising from interactions with domestic and overseas systems, particularly in enabling effective matching for watch list and other identification purposes, DIAC should assess the costs and benefits of broadening its biometric capability. Such a system would enhance its ability to use more of the available data effectively for matching purposes and give greater effect to the Government's requirement that the technology be *fully* interoperable with other countries' systems.

[118] An Inter-Governmental Agreement signed by all Australian police ministers, underpins the agency. The Ministerial Council for Police and Emergency Management - Police (formally known as the Australasian Police Ministers' Council) defines the agency's strategic directions and key policies, sets initiatives and appoints CrimTrac Board of Management members, who are responsible for overall agency management.

Conclusion

2.71 In 2004 DIAC was authorised to research and test ways of incorporating biometric technologies into existing visa and entry arrangements, and a capacity to store biometric images. The funding was for twelve months and was followed by a four-year initiative known as the *Biometrics for Border Control* initiative in 2005.

2.72 In considering its options for introducing biometrics, DIAC had conducted several tests and trials of biometric technologies. The Defence Science and Technology Organisation provided analyses into the effects associated with biometric enrolment and verification on DIAC.

2.73 In 2005, DIAC prepared a business case that identified sound reasons why a phased application of biometrics should be approved. Alternative non-biometric options to introducing biometrics were explored in earlier DIAC work but were not addressed in the business case. The scope and requirements were also apparent in the business case, but did not include a clear timeframe for the project development.

2.74 Also in 2005, DIAC prepared a cost-benefit analysis as part of the *Biometrics for Border Control* initiative and later identified key benefits to government from the introduction of biometrics. The expected benefits and costs are assessable, but to be meaningful, DIAC would benefit from a more structured approach to monitoring changes arising from its introduction of biometrics over time and evaluating the effectiveness of its chosen biometric solution in delivering its expected benefits. This is necessary to support management decisions about future directions in this area. DIAC's recently established evaluation and monitoring team is a useful first step in establishing an effective monitoring and evaluation capability.

2.75 A number of planning documents have also been prepared. Aside from a cross-agency Implementation Plan, DIAC also developed its own Implementation and Strategic Plans for the introduction of biometrics.

2.76 Success factors and critical dependencies were clearly identified in DIAC's planning documents. DIAC established clear timelines that set adequate review points for both business and IT deliverables. However, there have been delays in the delivery of specific capabilities primarily as a consequence of unmet dependencies on other related biometric or IT projects.

2.77 The wording of the *Migration Act 1958* expects DIAC decision makers to form judgements about the qualities ('integrity') of personal identifiers provided by DIAC clients. However, DIAC's policy guidance indicates that the intention was not that the qualities of personal identifiers themselves should be assessed, but rather that assessment should be of the *claims* being made by people about the identifiers (that the personal identifiers are theirs). In such a contestable area, there would be merit in DIAC considering the consistency between the legislation, as drafted, and the policy intent as part of a review of the legislation scheduled for 2008.

2.78 In approving the *Biometrics for Border Control* initiative, the Government decided that the four agencies should give priority to ensuring that the biometric technology introduced is fully interoperable with similar technology developed by other countries. Consistent with the approach taken by ACS and DFAT, DIAC has chosen the facial image as its primary biometric and has invested its resources accordingly. Its main counterpart overseas agencies (USA and UK) are implementing multi-modal biometric systems, involving faces and fingerprints.

2.79 Currently, DIAC has relatively limited capability to use other biometric data, such as fingerprints for matching purposes. Consequently, there is a risk that DIAC is unable to benefit fully from interactions with domestic and overseas systems. DIAC's early strategies have mainly focused on the use of face as a one-to-one matching capability. The current relatively limited fingerprint matching capability leaves the department in a position where it is unable to benefit fully from the international developments tending towards a broader use of fingerprints.

2.80 To maximise interactions with domestic and overseas systems, particularly in enabling effective matching for watch list and other identification purposes, DIAC should assess the costs and benefits of broadening its biometric capability.

Recommendation No.1

2.81 The ANAO recommends that, in order to support management decisions about future directions, DIAC implements a structured approach to monitoring changes arising from the introduction of biometrics over time, and evaluating the effectiveness of its chosen biometric solution in delivering its expected benefits.

DIAC response

2.82 Agree. DIAC agrees that it is now appropriate to develop structured monitoring and evaluation strategies. With the deployment of two biometric projects, and the establishment of the Identity Services Repository as a production database containing a substantial set of data, the department is positioned to assess the tangible benefits of these identity management tools. DIAC has already established an evaluation and monitoring team to measure the progress, outcomes and benefits of the identity management strategy, including the deployment of biometrics.

Recommendation No.2

2.83 The ANAO recommends that, in order to maximise potential for interoperability with overseas countries and Australian agencies and enable effective matching for watch-list and other identification purposes, DIAC assesses the costs and benefits of broadening its biometric capability to make more use of the main types of available data, including facial images and fingerprints.

DIAC response

2.84 Agree. We welcome the ANAO's recognition that a multiple biometric capability would enable DIAC to maximize its investment in biometric technologies. From the outset, DIAC has tested a range of biometric tools, including facial images, fingerprints and iris scans. DIAC's systems are being built to accommodate the collection and use of multiple biometrics and combinations of biometrics. DIAC acknowledges the importance of being able to deal with advances in technology and changes to our business and operating environments. The department will continue to explore the costs and benefits of various biometric solutions as well as any opportunities to efficiently expand our capability through our international collaborative efforts.

3. Governance Arrangements

This chapter examines the governance arrangements for DIAC's introduction of biometrics.

Introduction

3.1 Effective governance arrangements must be tailored to individual agency circumstances, based on a risk management approach that considers potential benefits and costs associated with activities that contribute to meeting specified objectives.[119]

3.2 In order to deliver its biometrics related projects successfully, DIAC's biometric initiatives need to be supported by an effective business and IT governance framework and sound funding arrangements. These assist in ensuring that the initiatives support business and IT goals and that the related risks and opportunities are appropriately managed.

3.3 This chapter assesses DIAC's governance arrangements for its biometric projects, in particular:

- DIAC's business governance;
- IT governance arrangements;
- IT project management; and
- funding arrangements.

Business governance

3.4 DIAC's governance frameworks for the introduction of biometrics have evolved over time. The department's initial governance structure, which has since changed, reflected the governance model of the four-agency initiative adopted in the *Development of Biometrics for Border Control 2005–2009*. Business governance arrangements, old and new, are outlined below.

Governance model of the four-agency initiative and DIAC's initial governance model

3.5 A governance model was developed by the four-agency initiative to ensure that: cross agency outputs supporting whole of government objectives

[119] ANAO *Better Practice Guide-Public Sector Governance*, Volume 1, July 2003, Canberra, p. 6.

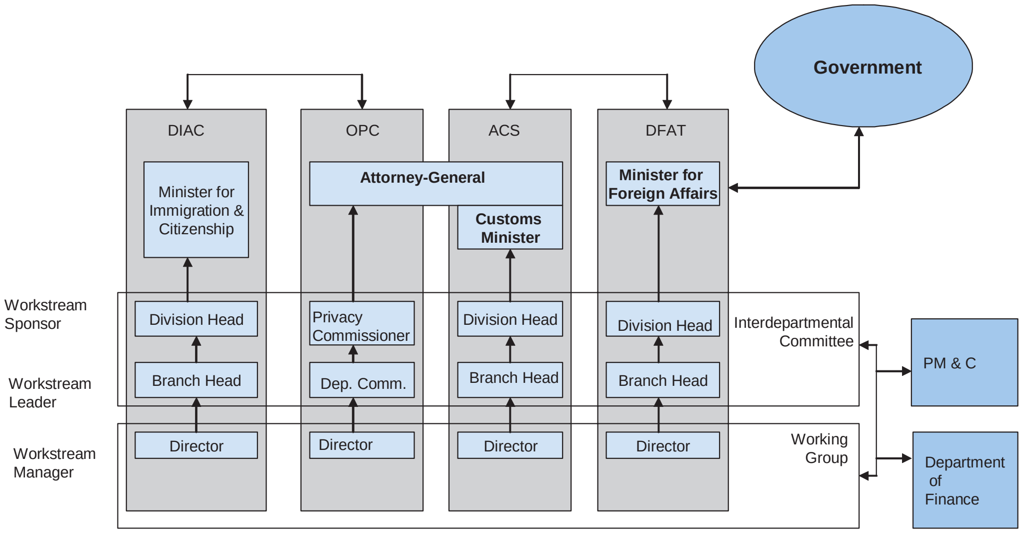
were met; and individual agency objectives were met within a whole of government framework.[120]

3.6 Under the four-agency initiative's governance model, program quality attributes (*program scope*, *management quality*, *schedule*, *risks* (changes), *outcomes* and *stakeholder support*), were to be measured and reviewed on a regular basis by agencies, and reviewed collectively by a Working Group on a monthly basis. The Working Group was to report to the Inter-Departmental Committee (IDC) on a quarterly basis prior to the regular report to the Cabinet Implementation Unit (CIU) in the Department of Prime Minister and Cabinet (PM&C).

3.7 Figure 3.1 illustrates the four-agency initiative's governance model. It covers DIAC's initial governance model for *Biometrics for Border Control*.

Figure 3.1

Governance model of the four-agency initiative



Source: ANAO based on the *Implementation Plan (2006–07) Development of Biometrics for Border Control 2005–2009.*

3.8 DIAC took over the responsibility of the working group and the IDC at the end of 2006. A review of the first IDC minutes coordinated by DIAC showed that only the *outcomes* were recorded. There was no documentation of discussion of other program quality attributes, particularly program risks or changes.

[120] Four-agency initiative, *Implementation Plan (2006–07) Development of Biometrics for Border Control 2005–2009*, 27 October 2006, p. 11.

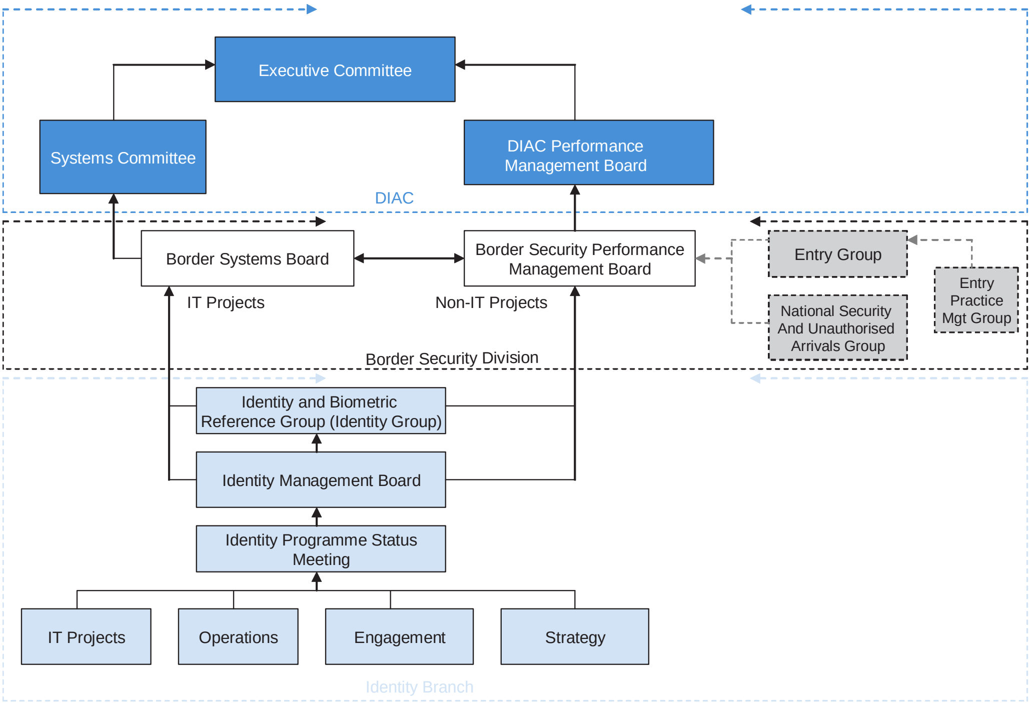
DIAC's new governance arrangements

3.9 In July 2007, DIAC's Identity Branch introduced new governance arrangements intended to ensure that its work aligned with broader DIAC planning processes and its Strategic Plan for identity management.[121]

3.10 DIAC undertook a review of its existing committees and governance, and implemented a revised governance structure to support the new organisational structure. DIAC Identity Branch's revised governance structure is set out in Figure 3.2.

Figure 3.2

DIAC Identity Branch's new governance structure


Executive Committee
Systems Committee
DIAC Performance Management Board
DIAC
Border Systems Board
Border Security Performance Management Board
IT Projects
Non-IT Projects
Entry Group
National Security And Unauthorised Arrivals Group
Entry Practice Mgt Group
Border Security Division
Identity and Biometric Reference Group (Identity Group)
Identity Management Board
Identity Programme Status Meeting
IT Projects
Operations
Engagement
Strategy
Identity Branch

Source: DIAC.

3.11 The Identity Branch's roles and responsibilities are discussed below.

Roles and responsibilities

3.12 DIAC's Identity Branch has responsibility for facilitating and monitoring the implementation of identity management solutions, including

[121] DIAC *Implementation Plan 2007–08*, *Identity Management in DIAC, Making the Identity Management Strategy a Reality,* 20 August 2007, p. 11.

biometrics, across the department's programs. The functions of the branch are set out in Figure 3.3.

Figure 3.3

Core functions of DIAC's Identity Branch

- Facilitate, guide and monitor the implementation of identity management across the department's business.
- Research, test and develop the required supporting biometric tools.
- Provide a range of ongoing identity management services.
- Develop an identity resolution capability.
- Manage and report on DIAC's contribution to whole-of-government identity initiatives, particularly the Biometrics at the Border capability and the National Identity Security Strategy.
- Develop processes and technologies that are compatible with Australia's key international partners.

Source: DIAC's Strategic Plan for Identity Management.

3.13 Initially, the Identity Branch comprised seven sections and its structure followed a traditional hierarchy approach where each section had responsibility and ownership of the branch's functions. In July 2007, DIAC implemented a new model for the branch structure. The sections were integrated into four groups: strategy; operations; engagement; and projects.[122]

3.14 The ANAO found that early planning documents clearly set out the responsibilities of the various sections. The current departmental Implementation Plan includes the responsibilities of the four groups and its new individual sections.

3.15 The ANAO considers the current organisational framework aligns and integrates the Identity Branch's individual projects to the rest of the department. In addition, there are clear accountability arrangements for all sections and teams within the Identity Branch that are reflected in the branch's planning documents (i.e. business plans and implementation plans).

Senior Responsible Officer (SRO)

3.16 The SRO plays an important role in giving visibility to the strength of executive-level support to the implementation of an initiative, considering funding issues that are relevant, providing delegations to the appropriate levels and considering whether the right people have been engaged.[123]

[122] The four groups cover eight sections: Business Engagement; Government Engagement; Projects Portfolio; GEM; Identity Services Operations; NIVA; Identity Resolution; and Document Examination.

[123] ANAO Better Practice Guide, *Implementation of Programme and Policy Initiatives*, 2006, p. 13.

3.17 DIAC advised that the head of the Identity Branch is the SRO for the introduction and implementation of biometrics. Although the Branch Head's roles and responsibilities are not documented in any of the planning documents, the ANAO considers that the position satisfies the role of an SRO.[124]

Risk management

3.18 Systematic risk management practices enable agencies to be confident that implementation has been designed to achieve government objectives most effectively.[125]

3.19 The ANAO found that the Identity Branch's Risk Register and Treatment Plan were sound. Risks were documented and updated, and had clear mitigation responsibilities. There was also high-level monitoring of risk management. For example, senior officers 'sign off' on the branch's Risk Management Plan, and this was monitored by the Divisional Strategic Assessment Unit (SAU).

3.20 The SAU advised that departmental risk management reporting requirements are currently being developed, in part, as a response to the Palmer and Comrie reports.

Performance information

3.21 The collection of performance information provides agency management and external stakeholders with the ability to monitor progress in implementing programs. It also assists in assessing whether outcomes, outputs and targets are achieved, and determining any changes that need to be made.

3.22 DIAC's Strategic Plan and Implementation Plan identified four key deliverables to affect the identity strategy, these include: organisational change via an identity change management strategy; an identity services capability; an identity resolution capability; and the biometrics at the border capability. The department also developed performance measures addressing the goals for each of these deliverables. Critical success factors are included, as discussed in paragraphs 2.34 to 2.37.

[124] The Identity Branch's organisational chart shows the Branch Head as the person accountable for the success of the implementation of the branch's policies and the person to whom the various section heads report.

[125] ANAO *Better Practice Guide-Implementation of Programme and Policy Initiatives Making Implementation matter,* October 2006*,* Canberra, p. 19.

3.23 In addition, the branch's new organisational structure includes a Governance, Evaluation and Monitoring (GEM) section which is intended to monitor most aspects of the branch's governance, accountability, evaluation, performance and continuous improvement functions.

3.24 DIAC has also reported quarterly to the Cabinet Implementation Unit (CIU).[126] The ANAO found that there has been an improvement in the quality and clarity of the CIU reports over time. Initially, the reports were brief and not transparent as to individual project progress. However, recent reports more clearly related to individual projects, highlighting achievements as well as actual delays and departures from the original proposals.

3.25 Overall, the ANAO considers that DIAC's business governance arrangements are sound.

IT governance

3.26 IT governance ensures that the agency's IT strategy is aligned with the agency business strategy, control structures are implemented and IT-related risks, resources and performance are managed.[127] The ANAO assessed whether DIAC has implemented an appropriate IT governance structure for its biometric projects.[128]

3.27 DIAC's current IT governance structure was introduced in late 2005, replacing and improving upon an existing structure. Figure 3.4 represents the IT governance committee structure.

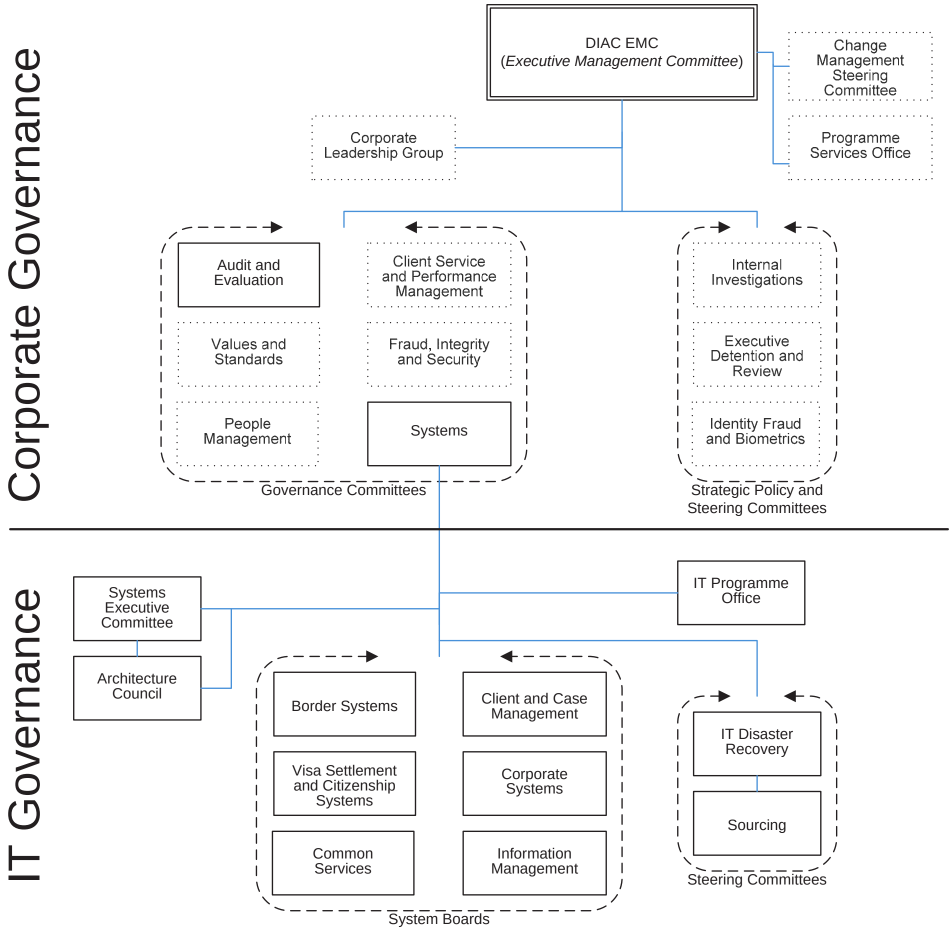
[126] CIU reports are intended to reflect the outcomes of the program or policy measures for a given period and the issues and outcomes to date.

[127] IT Governance Institute, 2007, *Control Objectives for Information and Related Technology (CobiT),* Version 4.1. Endorsed by the Information Systems Audit and Control Association (ISACA).

[128] The audit had regard to best practice for IT governance strategy (such as: National Computing Centre, 2005, *IT Governance—Developing a successful governance strategy*).

Figure 3.4

DIAC IT Governance Structure


Corporate Governance
DIAC EMC
(*Executive Management Committee*)
Change Management Steering Committee
Programme Services Office
Corporate Leadership Group
Audit and Evaluation
Values and Standards
People Management
Client Service and Performance Management
Fraud, Integrity and Security
Systems
Governance Committees
Internal Investigations
Executive Detention and Review
Identity Fraud and Biometrics
Strategic Policy and Steering Committees
IT Governance
Systems Executive Committee
Architecture Council
IT Programme Office
Border Systems
Visa Settlement and Citizenship Systems
Common Services
Client and Case Management
Corporate Systems
Information Management
System Boards
IT Disaster Recovery
Sourcing
Steering Committees

Source: ANAO based on DIAC documentation.

3.28 The current structure comprises of six Systems Boards, two Steering Committees, the Systems Executive Committee and Architecture Council. Systems Boards are responsible for overseeing specific systems within their defined business areas. All of the mentioned governance bodies advise and report to the Systems Committee.[129]

3.29 Biometric related projects report specifically to the Border Systems Board. The First Assistant Secretary Border Security Division (BSD) is the

[129] DIAC, 2006, *IT Governance Structure and Groups*.

chair. The Deputy Secretary Borders, Compliance and Technology Group chairs the Systems Committee.[130] The Committee provides the management interface between Corporate and IT governance structures.[131]

3.30 DIAC's IT Programme Office (ITPO) provides advice and facilitates the implementation and operation of IT governance and project management mechanisms.[132] The ITPO also provides advice and guidance to the Systems Committee on project, program and portfolio management issues.[133]

3.31 In addition, the Departmental Audit Committee (DAC) is a fundamental element of the governance structure. DAC provides independent assurance that a robust internal control structure is in place and outputs and activities are operating effectively, efficiently and lawfully.[134]

IT project reporting

3.32 In mid-2006, DIAC implemented the Clarity Project and Portfolio Management tool. Clarity provides project and portfolio management functions which assist DIAC in managing and monitoring projects.

3.33 DIAC's biometric related IT projects, the Identity Services Repository (ISR) and Detention Centre Rollout (DCR) projects, report through the IT governance structure, specifically to the Border Systems Board. The ANAO found that the ISR and DCR projects were providing project status information within the Clarity tool at least weekly, as required by the DIAC IT project management framework. The ITPO uses the Clarity tool to generate portfolio and project summary reports for both SfP and non-SfP projects.[135]

3.34 In addition, the ITPO prepares a report of 'Programme Risks and Issues' for use by the Systems Executive Committee. The ANAO found that project status information was presented to the committee, and that minutes were made of discussions of projects with a 'red' status.[136]

[130] Both the Border Systems Board and the Systems Committee meet monthly.

[131] DIAC, 2006, *IT Governance Structure and Groups*.

[132] The ITPO provides secretariat services to the Systems Committee, one of the Systems Boards (the Common Services Board) and the Systems Executive Committee.

[133] DIAC, 2006, *IT Governance Structure and Groups*.

[134] DIMA, *2005–06 Annual Report*.

[135] Reports prepared and provided to the Systems Executive Committee include a: SfP Project Summary Report; Non-SfP IT portfolio status summary; and Red Status Report, which provides a listing of projects that have reported a red status on any project elements, such as risks, issues, milestones, finances or overall.

[136] The ANAO reviewed Systems Executive Committee meeting minutes from January to June 2007.

Project Risk and Issue Transparency

3.35 The ANAO found that highly rated risks were being reported to the Systems Executive Committee. However there was limited evidence to show that specific risks in relation to biometric IT projects were being discussed in meetings of the Border Systems Board.

3.36 The ANAO found that the limited details recorded in relation to discussions held on project status or projects that had highly rated risks or issues, made it difficult to ascertain: which project risks and issues had been presented to the Border Systems Board; whether they were discussed or assessed in a timely manner; or any actions required for escalation or resolution.

3.37 The ANAO considers that better documentation of meeting minutes would strengthen DIAC project risk and issue transparency, particularly by providing evidence that project risk and issues were presented, discussed and assessed; and of actions raised to escalate or resolve reported risks or issues.

Involvement by DIAC Internal Audit

3.38 Better practice indicates that benefit can be gained from early and ongoing involvement of the Internal Audit function in IT system development initiatives.[137] In the course of such involvement, Internal Audit may provide guidance and assurance over controls and processes employed, for example in relation to: IT project planning, monitoring and control; software quality assurance; and the design of application controls.

3.39 The ANAO examined DIAC Internal Audit's involvement in biometric related IT projects, specifically the ISR and DCR. The ANAO found that:

- no internal audits of the ISR and DCR projects were conducted during 2005–06 or 2006–07;
- the Border Systems Board meeting minutes between the period of January and June 2007 showed no attendance by an Internal Audit representative; and
- Internal Audit had not been involved in the systems development phases of the ISR or biometric solution, specifically.

[137] ANAO, 2007, *Better Practice Guide: Public Sector Internal Audit—An investment in assurance and business improvement*, p. 22.

3.40 DIAC advised that the Internal Audit Program is developed having regard to the department's annual risk profile, management priorities, previous internal and external audit coverage, planned external audits, management initiated reviews, an additional broader environmental scan, and available resources. DIAC also advised that it will continue to encourage the strategic use of expertise that resides within the internal audit area when undertaking major IT systems development, having given the necessary consideration to the costs and benefits of any such activity.

IT project management

3.41 An IT project management framework aims to ensure the delivery of project results within agreed-upon time frames, budget and quality constraints. It also defines the project scope and method.

3.42 The ANAO assessed[138] whether DIAC's biometrics related IT projects were:

- supported by an effective framework for project management; and
- effectively and appropriately applying aspects of DIAC's IT project management framework and processes.

DIAC IT project management

3.43 DIAC commenced effort on a number of biometric projects, such as the Biometrics Testing Facility, Biometric Capture Trials, and Identity Services Repository in the period spanning 2004 to 2005. DIAC had not implemented a corporate IT project management framework at that time. However, processes did exist whereby projects were initiated and approved, and IT resources budgeted and assigned to project activities.

3.44 In late 2005, DIAC recognised the opportunities afforded by the use of widely accepted project management standards and better practice and formally implemented an IT project management framework. DIAC's IT Project Management Framework,[139] which details the department's project

[138] The audit had regard to a number of better practice sources from the project management discipline. This included the internationally accepted standard known as the Project Management Body of Knowledge (PMBoK). PMBoK has International Standards Organisation 9001 certification and is an American National Standards Institute standard.

[139] DIAC, 2006, *IT Project Management Framework*, Version 1.2. The famework specifies the roles and responsibilities of all project stakeholders; project control mechanisms; IT project lifecycle; and approval and governance processes that apply to all IT projects. It also provides project management support and advice (including training and mentoring) to project managers, and is responsible for authoring and maintaining documentation relating to the project management framework and processes.

management standards and techniques, is largely based on the Project Management Body of Knowledge (PMBoK). The agency's IT Project Management Framework also includes a Requirements Management Policy for all its IT projects.

3.45 DIAC established the ITPO (see paragraph 3.30) in order to centralise and coordinate the management of projects. The ITPO provides IT project, program and portfolio management services that enable projects within the department to deliver outcomes that align with the DIAC Plan and DIAC's strategic themes.[140] The ITPO has developed an integrated suite of project management tools, templates and guides for use by IT project teams, known as the 'Project Management Reference Suite'.[141]

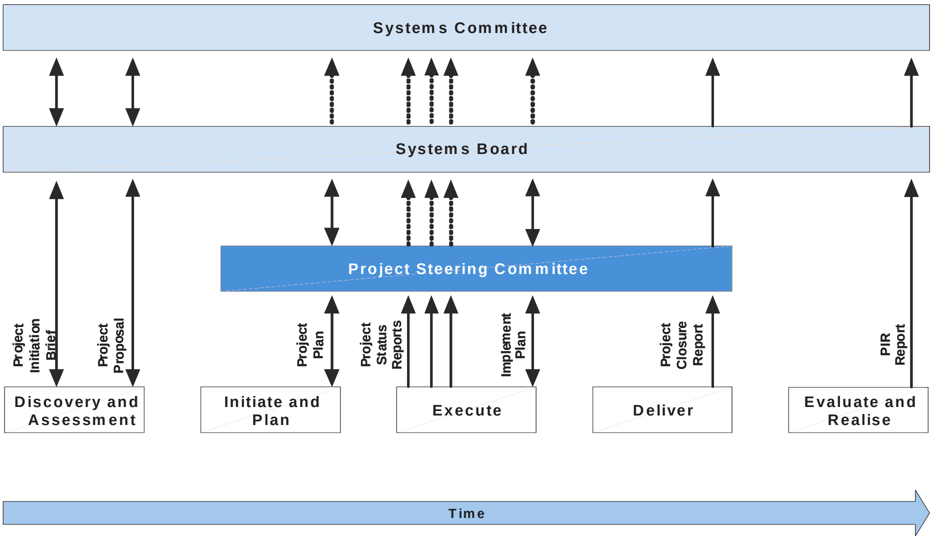
3.46 As previously noted (see paragraph 3.32) DIAC implemented the Clarity Project and Portfolio Management tool in June 2006. DIAC uses the tool to manage all SfP projects and some other non-SfP IT projects. DIAC has mandated the use of Clarity, and progressively enters new projects into Clarity as the Systems Committee approves them. The DIAC IT project management process is integrated with the IT Governance process, as represented in Figure 3.5.

[140] DIAC Intranet, IT Programme Office (ITPO) homepage.

[141] The Suite is made available to all stakeholders through the DIAC intranet. Key documents within the suite include the IT Project Management Framework and the IT Project Management Process Guide. The IT Project Management Process Guide describes the processes and activities to be undertaken by Project Managers to ensure that their project meets its schedule, budget and quality criteria.

Figure 3.5

Integration of IT Governance and Project Management



Source: DIAC IT Project Management Process Guide version 3.0.

IT project management within biometric projects

3.47 The ANAO assessed whether DIAC's biometric related IT projects were effectively and appropriately applying aspects of DIAC's IT project management framework and processes. Specifically, the ANAO examined the ISR and DCR projects. Both projects commenced prior to DIAC's implementation of its IT project management framework.

Identity Services Repository (ISR) project

3.48 The ISR project was established in mid-2004. Several project phases have been successfully completed with more phases forecast through to 2009.

3.49 DIAC has commenced applying aspects of the new IT project management framework and processes to the ISR project. DIAC approved the ISR project in 2004, and the ANAO noted that the project has developed a Project Management Plan.[142]

3.50 The ANAO found that the project team uses the Clarity tool to report weekly on project status, ensuring that project status, risks and deviations are reported to the relevant governance entities.[143]

[142] The ANAO did not assess project artefacts such as the Project Proposal and Project Initiation Brief, as these were not required at the time.

[143] The finances, resources, milestones, risks and issues are being tracked. A weekly status report, which addresses these areas, is provided internally to the Identity Projects Portfolio manager.

Detention Centre Rollout (DCR) project

3.51 The DCR project commenced in June 2005 and is scheduled for completion by December 2007.[144]

3.52 The DCR project team has been tasked with delivering the project under a tight timeframe, while meeting new conditions imposed by the Systems for People program, and while working in an organisation undergoing change and renewal. The ANAO found that the project team was also under-resourced, due to the loss, and non-replacement, of key project team members.

3.53 DIAC has commenced applying aspects of the new IT project management framework and processes to the DCR project. The Project Management Plan has been maintained and mandatory project artefacts[145] have been developed throughout the life of the project.[146]

3.54 The ANAO considers that effective mechanisms have been implemented in relation to project control and monitoring.[147] The ANAO considers that the DCR project has established and implemented adequate controls to ensure that project status, risks and deviations are reported to the relevant governance entities.

3.55 However, the ANAO found that the DCR project is not complying fully with the IT project management methodology. For example:

- a Project Quality Log was introduced in April 2007 as a new mandatory project requirement. At the time of the audit, the DCR project had not had the opportunity to use this template; [148] and
- a Communications Log, a recommended mechanism for control was established in March 2007 but was not used during the project.

[144] DIAC, 2007, *SFP070 DCR Stage 2 Project Management Plan*, Version 2.

[145] Mandatory project artefacts such as the Project Initiation Brief, Project Management Plan and Risk Management Plan.

[146] The Systems Committee did not require completion of a Project Proposal, which is usually a mandatory artefact.

[147] Mandatory project artefacts such as Project Risk and Issues Logs have been developed, and are maintained weekly. Finances, resources, milestones, risks and issues are being tracked. The project prepares a weekly status report which addresses these areas and provides this internally to the Identity Projects Portfolio manager. A weekly Project Status report is also produced in Clarity.

[148] The DIAC IT project management policy requires that quality activities associated with acceptance of project deliverables be recorded in the Project Quality Log.

3.56 Documentation of key decisions, and reasons for the decisions, are core elements of sound project management. However, the ANAO found that project team and stakeholder discussions, and decisions, were not being adequately recorded. The project team established a Decision Register at the onset of the project, within which decisions were to be recorded. However, this register was not being maintained.

3.57 The ANAO considers that, in this case, establishing and maintaining the Project Quality and Communications logs and the Decision Register would have provided documentary records of the tasks undertaken. This is important in managing relationships with various stakeholders, especially in a long-term project where 'corporate memory' can otherwise be lost. Also, the act of maintaining such records can act as a reminder to the project team to undertake the planned quality assurance and communications tasks.

3.58 The ANAO suggests that future biometric related IT projects: ensure compliance with DIAC's IT project management framework, giving attention to completing ongoing mandatory and recommended project activities; and strengthen project administration in relation to record keeping, ensuring that decisions made during the life of the project are documented.

3.59 Overall, the ANAO considers that the IT project management framework, processes and tools DIAC implemented in late 2005 are sound. The biometric IT related projects, specifically the ISR and DCR projects, are generally applying the DIAC IT project management framework. There are, however, opportunities to improve compliance with the process and to improve on the level of project administration, particularly in relation to the recording of decisions throughout the life of projects.

Funding arrangements

3.60 DIAC's introduction of biometrics is to be delivered through a series of projects. The projects are based on, or have been affected by, a series of decisions announced by government in May 2004, May 2005 and May 2006.[149]

3.61 The ANAO assessed: the transparency and timeliness of funding allocations to the biometrics projects; the reliability of financial data for reporting purposes; and the effectiveness of DIAC's management of the additional revenue generated by the Visa Application Charge (VAC) increase in meeting the goal of offsetting the costs of DIAC's introduction of biometrics.

[149] The government decisions are outlined in more detail at paragraphs 2.42-2.45.

Transparency and timeliness of funding allocations

3.62 To be effective in managing complex multi-year projects, project managers must have a clear understanding of their available budget, and be confident that these funds will be available when required.

3.63 The ANAO found that, at the time of the audit, there was considerable uncertainty in DIAC's Identity Branch as to its funding base. For example, there was uncertainty arising from the Government's decision in May 2005 to merge later stages of the ISR project with DIAC's broader Systems for People (SfP) project—as a result the ISR allocation was transferred from Identity Branch to SfP. However, the Identity Branch was unsure of the details of this decision and was uncertain whether it had received fully an appropriate budget allocation in 2006–07. The ANAO's enquiries confirmed the distribution of funds and resulted in the clarification of allocations to the various DIAC areas for the key biometric projects.

3.64 The ANAO also found that there was a substantial delay in finalising the 2006–07 internal allocations across DIAC—the Identity Branch advised that it did not receive advice of the outcome of a mid-year budget review until February 2007. DIAC advised that, for the biometrics program, the delay had had a substantial business impact on the biometrics program—it had created uncertainty, in particular, caution in entering into spending commitments, such as contracts, in the absence of confidence about the amount of funds available for use.[150] DIAC has separately received advice about the need to improve the transparency and timeliness of internal budget allocations.[151]

Reliability of financial data for reporting purposes

3.65 DIAC's systems enable reporting against project codes. Consequently, the department should be able to readily and accurately report on the monies allocated and expended on its biometrics projects. However, to be effective as reporting tools, these codes need to align with the projects approved by government.

[150] DIAC advised that it had deferred lower priority projects, such as developing the biometric 'watch list' and establishing links with the DFAT and NZ passports databases. DIAC also advised that there had been some unexpected benefits and opportunities arising from the delay in commencing and progressing some projects. For example, DIAC is exploring with other countries (such as United Kingdom, Canada and the United States of America) the feasibility of joint biometric capture, whereby the participating countries could capture biometrics from visa applicants on behalf of each other. This would result in much more efficient data capture arrangements, and reduce the need for offshore deployment of biometric enrolment equipment by Australia, which had been anticipated in the 'Fixed and Deployable' project.

[151] Paul Hickey, 2007, *Department of Immigration and Citizenship: Review of Governance*, pp 18–19, 29.

3.66 The ANAO found that DIAC has created *allocation* codes that broadly correspond with the biometrics projects approved by government. However, the *expenditure* codes created by DIAC in its systems are not well aligned with the projects approved by government. For example, some biometrics 'projects' in DIAC's expenditure data represent an amalgam or portion of the approved projects, while funds nominally for 'projects' aligned with the Government decision have been used for different activities.

3.67 Furthermore, there are limitations in the project expense data that reduce its accuracy for reporting purposes. For example, many expenses incurred by DIAC's Identity Branch, particularly employee expenses, were not recorded against a particular project. In 2005–06, around 35 per cent of the Branch's operational costs were not recorded against a particular project, rising to over 54 per cent in 2006–07.

3.68 Consequently, the ANAO considers that any project level reporting based on the project expenses code data is likely to be substantially inaccurate.

3.69 Notwithstanding the limitations in DIAC's project-level expenditure data, it is possible to report on the aggregate allocations and expenditure for the biometrics projects. The ANAO's analysis shows that in total, the biometrics projects approved by government come to around $83.2 million over the period 2003–04 to 2009–10,[152] of which $80.505 million was additional funding.[153] The ANAO's analysis shows that, overall, DIAC had recorded expenditure of around 84 per cent of its allocations to the end of 2006–07 on a pro-rata basis.[154]

3.70 Overall, the ANAO considers that more transparent and timely communication of allocation decisions and better data on project expenditures would help in both managing the biometrics projects and in accounting for the use of funds approved by government for DIAC's biometrics initiatives.

The cost of introducing biometrics in DIAC was offset by a five per cent increase in the Visa Application Charge (VAC)

3.71 VAC is a tax imposed on visa applicants by the *Migration (Visa Application) Charge Act 1997*. Under the *Migration Act 1958*, a non-citizen who

[152] Figures include indexation, depreciation, and disaster recovery.

[153] In May 2004, the government announced $4.396 million in new capital and operating funding for 2004–05. The department also internally funded $3.184 million and incurred $0.734 million in depreciation costs in 2004–05.

[154] Excluding overheads, depreciation and corporate priorities (indexation). DIAC advised that underspent capital funds have been carried forward for future use.

makes a valid application for a visa is liable to pay VAC. The Migration Regulations, authorised by the *Migration Act 1958*, specify the amounts payable (which vary among visa types).[155] VAC raises most of the revenue DIAC collects.[156]

3.72 The Government has the discretion to set VAC for any type of visa at any level it chooses, provided that level remains below a prescribed VAC limit.[157] Because VAC is a tax, all revenue is paid into the Australian Government's Consolidated Revenue Fund (CRF). Decisions on how to disburse the VAC revenue are ones for Parliament through the appropriation process. There is no necessary connection between the amount of funding DIAC receives in appropriations from the CRF and the amount of VAC revenue paid into CRF.

3.73 In May 2005, the Government announced that it had decided to increase VAC on selected visa types by five per cent to offset the costs of DIAC's biometrics program over the four year period 2005—06 to 2008—09.[158] The increase in VAC was not imposed on Tourist, Visitor or Student visas as this was considered likely to attract significant criticism from the relevant industry groups. The revenue raised by the VAC increase would also be used to offset costs of the Office of the Privacy Commissioner relating to the introduction of biometrics in DIAC, DFAT and ACS.

3.74 DIAC provided government with estimates of the additional revenue based on forward projections of visa application numbers. The VAC charges were increased on the selected visa types from 1 July 2005.

Monitoring the additional revenue generated by the VAC increase

3.75 The ANAO assessed the effectiveness of DIAC's management of the additional revenue generated by the VAC increase in meeting the goal of offsetting the costs of DIAC's biometrics program.

[155] See s. 45 of the *Migration Act 1958*.

[156] In 2005–06 VAC raised an estimated $498.9 million (see ANAO Report No.7 2006–07, *Visa Management: Working Holiday Makers*, p. 97).

[157] The *Migration (Visa Application) Charge Act 1997* provides for the indexation of a parameter known as the 'visa application charge limit', a ceiling on the amount of charge that may lawfully be prescribed in the regulations. This limit, originally set at $12 500, and now $15 585, is very much greater than most VAC rates (see ANAO Report No.7 2006–07, *Visa Management: Working Holiday Makers*, pp. 99-100).

[158] The Hon. Alexander Downer MP, Minister For Foreign Affairs; Senator The Hon. Amanda Vanstone, Minister for Immigration, Multicultural and Indigenous Affairs; Senator The Hon. Christopher Ellison, Minister for Justice and Customs, 10 May 2005, *Joint Media Release: Development Of Biometric Technology For Border Control.*

3.76 The ANAO found that DIAC monitors overall VAC revenue and examines this twice yearly, as part of the budget cycle. However, DIAC did not specifically monitor the additional revenue raised for the Australian Government by the five per cent VAC increase on selected visa types from 1 July 2005.

3.77 The ANAO analysed DIAC's original projections for additional VAC revenue, and also re-visited the amount of likely revenue to be generated in light of actual application numbers for 2005–06 and 2006–07 and updated estimates for the forward years.

3.78 The ANAO found that DIAC's original projection of additional revenue underestimated the likely additional revenue by $1.59 million (3.7 per cent) because it was based on the raw adjusted VAC rates, rather than the rounded rates actually paid by visa applicants.[159] The ANAO also found that there has been widespread variation in visa application rates from the original projections. While the number of applications for some visa types has been lower than expected,[160] applications for the high volume/high value visa types such as spouse, skilled independent, skilled—independent overseas student and Working Holiday Makers have been much higher than originally projected. Taken together, the ANAO estimates that DIAC's original projection underestimated the additional revenue by around $6.65 million (15.3 per cent).

3.79 The ANAO considers that there is likely to be substantially more VAC revenue paid into the CRF than originally projected—in essence, a 'windfall' gain to the Australian Government. Because it did not monitor the additional revenue generated by the VAC increase, DIAC was unaware of the excess revenue accruing to the CRF.

3.80 Further, DIAC advised that the Government decided in 2007─08 that the VAC increase would be ongoing, overturning a repeal process that previously applied. Consequently, at the end of the four-year period, certain visa applicants will continue to pay the higher VAC despite more than sufficient revenue having already been generated to offset the expected costs of the biometrics program.

[159] VAC rates were increased by five per cent and then rounded to the nearest $5 as is usual DIAC practice. For example, the previous Spouse (Residence) VAC was $760. An increase of five per cent raised this to $798, which was then rounded to $800. The latter figure should have been used in calculating the additional revenue.

[160] Some visas have also been abolished or replaced.

3.81 DIAC advised that, unlike previous instances, it had not been asked by Government to monitor the additional revenue generated by this particular VAC increase. However, the ANAO considers that closer monitoring would have helped the department to better manage the risks of not meeting the Government's intention to 'offset' the costs of the program through the VAC increase.[161]

Conclusion

3.82 The four agencies involved in the *Biometrics for Border Control* initiative developed a governance model aimed at ensuring cross-agency outputs supporting whole of government objectives were met, and individual agency objectives aligned with the whole of government framework. Similarly, DIAC's Identity Branch introduced new governance arrangements to ensure alignment with broader DIAC planning processes and its strategic plan for identity management.

3.83 DIAC's Identity Branch has responsibility for the agency's implementation of identity management solutions, including biometrics. The Branch's current organisational framework aligns and integrates the individual projects to the rest of the department. There are clear accountability arrangements within the Branch.

3.84 DIAC's current IT governance structure was introduced in late 2005. Systems Boards are responsible for overseeing specific systems within their defined areas. All IT governance bodies advise and report to DIAC's Systems Committee. DIAC's highly rated IT risks were reported to DIAC's Systems Executive Board. However, there were limited details recorded of specific risks in relation to biometric IT projects discussed in meetings of DIAC's Border Systems Board.

3.85 DIAC's biometric related IT projects, the Identity Services Repository (ISR) and the Detention Centre Rollout (DCR) projects, report through the IT governance structure. Both the ISR and DCR projects were providing project status information, as required by the DIAC IT project management framework. However, more comprehensive documentation of key decisions, and reasons for the decisions would strengthen project design and

[161] There are two main risks: first, if the amount of revenue generated is substantially less than projected, there will be an unexpected net drain on CRF. Conversely, if the amount of revenue generated is substantially more than projected, there will be a net boost to CRF. In both cases, the Governments intention will not be met.

administration. DIAC's Internal Audit has had little involvement in the development of the biometric systems.

3.86 At the time of the audit, there was uncertainty in DIAC's Identity Branch about the allocation of funds to the biometrics projects—however this was clarified as a result of the audit. While it is possible to report on aggregate allocations and expenditure for the biometrics projects, DIAC's practices in recording project level expenditure were inadequate, meaning that any project-level reporting for the $83 million biometrics projects is likely to be substantially inaccurate. Going forward, the ANAO considers that more transparent and timely communication of allocation decisions and better data on project expenditures would help in managing the biometrics projects and in accounting for the use of funds approved by government for DIAC's biometrics initiatives.

3.87 The goal of offsetting the costs of the biometrics initiatives by raising the Visa Application Charge (VAC) by five per cent on certain visa types could have been better managed and monitored. The ANAO found that there is likely to be substantially more revenue raised than originally projected—in essence a 'windfall' gain to the Australian Government. Closer monitoring would have helped the department to better manage the risks of not meeting the Government's intention to 'offset' the costs of the program through the VAC increase.

4. Administrative Arrangements

This chapter examines DIAC's administrative arrangements, including its IT system development for the introduction of biometrics.

Introduction

4.1 Effective implementation requires appropriate administrative arrangements. This chapter assesses key DIAC administrative arrangements for the introduction of biometrics, including:

- development of guidance and training for staff;
- mechanisms for assuring privacy; and
- IT system development methods and processes.

Guidance and training

4.2 Appropriate guidance, together with a thorough assessment of training needs, are important considerations for successful implementation and to ensure that there is consistent application of rules by appropriately skilled and supported staff.

Guidance for staff

4.3 DIAC has prepared detailed guidance on client identity matters, including biometrics, for staff for inclusion in DIAC's Procedures Advice Manual (PAM). At the time of the audit, much of the guidance was in draft form.

4.4 The ANAO found that the guidance provides sound advice for staff to use in dealing with personal identifiers and related information. However, finalisation of comprehensive guidance has not been timely. While there had been a delay finalising the PAM guidance, other, less comprehensive, guidance had been in existence for some time.

- DIAC staff advised the ANAO that the finalisation of the PAM guidance should have occurred earlier, to keep pace with the development of DIAC's identity management approach.
- The ANAO noted that there had also been delays in up-loading completed PAM guidance onto LEGEND (the system through which staff can access PAM).

4.5 The ANAO considers that when completed and available for staff, the PAM guidance would benefit from being accompanied by a structured performance monitoring and feedback strategy. This would provide DIAC with assurance that the guidance is useful to staff, is being used consistently and appropriately (consistently establishing identity to an appropriate level using appropriate methods/tools), and that this is delivering the benefits expected. The ANAO notes that DIAC's National Quality Assurance Framework may provide a suitable platform for obtaining this assurance (see paragraph 4.30).[162]

Training

4.6 At the time of the audit, most of the training and reference materials regarding identity management were still being developed. DIAC had prepared an Identity Management Training Plan 2007–2010 that maps out specific training initiatives for the Identity Branch. The plan aims to ensure that staff acquire the knowledge and skills to perform their job through a coordinated, comprehensive and timely identity management training schedule.[163]

4.7 The release of relevant training and reference materials is intended to coincide with the progressive roll-out of business deliverables between 2007–2010. DIAC advised that after ANAO's fieldwork for the audit was completed, the identity management training in relation to the new Citizenship Test had been developed and delivered. DIAC also advised that an Identity Branch Orientation package was being developed and would be in place soon.

4.8 The ANAO considers DIAC's training plan for identity management to be adequate.[164] The training plan is particularly beneficial as the department reviews the alignment of its current skill-set to actual skills and training required.

[162] DIAC's National Quality Assurance Framework was approved in August 2006. The framework's objectives are to: help business areas understand the basic principles of quality assurance; provide guidance on the design and review of quality assurances processes; and promote the implementation of quality assurance across DIAC. See: <http://www.immi.gov.au/media/publications/palmer-progress/_pdf/quality-assurance.pdf>, [accessed 14 September 2007].

[163] DIAC, *Identity Management Training Plan 2007–2010,* August 2007. Some staff within the Identity Branch had already received some form of training and exposure with regards to identity. For example, key members of the Document Examination section have the technical expertise to detect fraudulent identification documents. Similarly, some staff of the National Identity Verification and Advice (NIVA) section have technical knowledge of the operations of Cognitec, a standalone facial recognition software package that is used by DIAC.

[164] The plan includes training activity summary sheets, key principles, resources and the need to undertake evaluation and training as required.

Assuring privacy

4.9 The *Migration Act 1958* and *Australian Citizenship Act 1997* set out requirements in relation to accessing, disclosure, retaining and destroying personal identifiers and related information—collectively known as 'identifying information'.

4.10 The ANAO sought to determine whether DIAC had developed a robust framework for administering these requirements.

Accessing and disclosing identifying information

4.11 Under the *Migration Act 1958*[165] and *Australian Citizenship Act 1997*[166] permitted reasons for access include: the purposes of collecting personal identifiers (set out in Appendix 5) as well as for administrative, matching and legal reasons. Permitted reasons for disclosure are similar to the Information Privacy Principles in the *Privacy Act 1988*, and include: data matching; access by system administrators; disclosure to the person to whom it relates; and where disclosure is required by law. Unauthorised access and disclosure are offences against both Acts.

Access to identifying information

4.12 In order to support information privacy, access to identifying information should only be made by authorised personnel for appropriate reasons. Further, loss or misuse of data has serious potential reputational risks for agencies that hold large quantities of identifying information.

4.13 The ANAO found that DIAC has designed its Identity Services Repository (ISR) so that access is based on a person's 'position number'. DIAC advised that the system will contain an audit trail of persons accessing identifying information.

4.14 DIAC was unable to provide evidence of actions taken to ensure that access to identifying information was only by authorised officers. Such actions could include:

- monitoring use of position numbers to ensure that they are only used by the person to whom they are assigned;
- ensuring position numbers are properly authorised under law; and

[165] Sections 336 C-D and 336 E-FD.

[166] Sections 42 and 43.

- ensuring position numbers are kept up-to-date.[167]

4.15 The ANAO also found that there is no monitoring process, active or planned, to provide assurance about the appropriateness of access to identifying information. The ANAO considers that DIAC should develop a strategy for obtaining reasonable assurance about both the authority for a person to access identifying information and the appropriateness of access by authorised persons.

Use of identifying information disclosed by DIAC to third parties

4.16 The *Migration Act 1958* and *Australian Citizenship Act 1997* set out arrangements for disclosure of identifying information. The *Migration Act 1958*, in particular, sets out arrangements for disclosure of identifying information to Australian agencies, individuals, the general public and foreign countries, foreign bodies and international organisations.[168] The ANAO reviewed the arrangements in respect of the *Migration Act 1958*.

4.17 The ANAO found that the protections in the *Migration Act 1958* surrounding access to, and disclosure of, identifying information, do not extend to the third parties to which DIAC discloses information. Consequently, DIAC advised that it is beyond its control to ensure that there is/will be no inappropriate use or disclosure of identifying information by the agencies to whom it discloses the information.[169]

4.18 For example, DIAC has a Memorandum of Understanding (MoU) with the Australian Federal Police (AFP) for the exchange of identifying information.[170] The MoU makes it clear that information exchanged is to be 'handled in accordance with applicable privacy laws', including the *Privacy Act 1988*.[171]

4.19 The caveats in Memoranda of Understanding are not binding on the parties to the MoU. Also, the general protection afforded by Australian privacy

[167] It was not within scope of this audit to review DIAC's position numbers.

[168] The whilom Minister for Immigration, Multicultural and Indigenous Affairs prescribed a wide range of Australian and foreign bodies and international organisations. See Commonwealth of Australia, Special Gazettes Nos S11 and S12, 25 January 2006.

[169] DIAC could not advise how many disclosures of identifying information had been made, stating however that there have been 'many', the majority of which 'would have been hard copy photos being disclosed for the purposes of identifying someone.'

[170] This allows exchanges of identifying information to occur between these two agencies if it is for one of the lawful functions of one of the agencies.

[171] *Memorandum of Understanding—AFP and DIMA—Exchange of Identifying Information*, signed 26 October 2006 (DIAC), and 1 December 2006 (AFP), sections 2, 7 and 8.

legislation, such as the *Privacy Act 1988* to personal information is not universal, and does not extend to overseas agencies to which DIAC may disclose identifying information.

4.20 The ANAO found that, in the case of the MoU between DIAC and the AFP, there is no mechanism for each party to notify the other party when information obtained from one party is disclosed to a third party or to document this disclosure. Further, there is no mechanism in the MoU to provide assurance that the protections applying to information disclosed by DIAC to the AFP would also apply if this information were to be on-disclosed by the AFP to another agency.

4.21 The ANAO considers that, while DIAC has limited capability to ensure identifying information disclosed by DIAC to third parties is appropriately protected, stronger provisions in its MoUs would provide some further assurance in this regard.

Assurance that disclosures are appropriately documented

4.22 It is DIAC policy that officers must make a file note about any disclosure of identifying information they have made under Part 4A of the *Migration Act 1958*.

4.23 DIAC advised that it is working on ensuring there is an audit trail for ISR usage and the fingerprint collection. However, as the file notes may be made in other systems,[172] the ANAO considers that such a trail will be of limited value for monitoring purposes. Consequently, the ANAO found that there is no effective process to provide assurance that disclosures of identifying information by DIAC staff are appropriately documented.

Retaining and destroying identifying information

4.24 The *Migration Act 1958* and *Australian Citizenship Act 1997* set out arrangements for the retention and destruction of identifying information. Both Acts make it an offence if the 'responsible person':

> fails to destroy the identifying information as soon as practicable after the person is no longer required under the *Archives Act 1983* to keep the identifying information.[173]

[172] Under policy, the file note can take the form of a case note on the Integrated Client Services Environment (ICSE) or Immigration Records Information System (IRIS) or other appropriate departmental database.

[173] *Migration Act 1958* (Section 333K (1)(e)) and *Australian Citizenship Act 1997* (Section 45 (1)(b)). DIAC was unable to identify who the 'responsible person' was for the purposes for these provisions.

4.25 While there is a general requirement in the Acts to destroy identifying information, exceptions include:

- a general exemption for height and weight measurements, facial photographs, signature, and related information; and
- in the case of the *Migration Act 1958*, the indefinite retention of identifying information for certain persons.[174]

4.26 The ANAO found that these exceptions mean that DIAC is authorised to retain indefinitely virtually all of the biometric information it is currently planning to collect.[175]

DIAC's records disposal authority

4.27 Under the *Archives Act 1983*, Australian Government agencies can enter into an arrangement with the National Archives of Australia, known as a 'records disposal authority' (RDA), that sets out creation, maintenance, retention or destruction actions to be taken in relation to existing or future records.[176]

4.28 DIAC considers that its current RDA[177] does not adequately address the disposal of identifying information.[178] A review of DIAC's RDA has been underway since 2003.[179] DIAC advised that it has included disposal of identifying information in the review of the RDA.[180]

Process to ensure that identifying information is not retained any longer than is appropriate

4.29 DIAC's current RDA provides for the disposal of records one year after 'the action is completed'. During the audit, DIAC advised that it considered that 'retention of a client's photograph for longer than one year would be warranted.' DIAC also advised that it was 'looking at ensuring that dates of entry of data are flagged'.

[174] Such as people who have been in detention, had a visa refused or cancelled, overstayed, been deported or removed, or committed an offence against the Act.

[175] Information such as biometric photographs from a range of visa and citizenship applicants, as well as fingerprints of people in immigration detention.

[176] See <http://www.naa.gov.au/recordkeeping/disposal/disposal.htm>.

[177] RDA 902.

[178] In June 2006, DIAC received internal legal advice that 'it would seem sensible to develop a disposal authority that covers the whole field of identifying information.

[179] DIAC has an RDA which was first issued in 1991 and amended in 2000.

[180] DIAC was unable to advise on the timeframe for completion of the review of the RDA, stating that 'Systems for People issues are making them [the records management area] reassess their priorities'.

4.30 The ANAO considers that date-stamping identifying information would be a useful first step in a process to actively monitoring the retention of identifying information. Following this, the department would have to institute monitoring processes to identify aged identifying information for destruction.

4.31 In the absence of these processes, DIAC currently does not have any means to assure itself that identifying information is not retained any longer than is appropriate.

DIAC can retain data about destroyed records

4.32 Both the *Migration Act 1958* and *Australian Citizenship Act 1997* specify that destruction of identifying information involves the physical destruction of personal identifiers,[181] and the destruction of any means of linking other information[182] with the person to whom it relates.[183]

4.33 Consequently, the Acts enable DIAC to retain some secondary information, so long as it cannot be linked to the person to whom it relates.

Implementing recommendations of the Office of the Privacy Commissioner

4.34 The four-year *Biometrics for Border Control* of May 2005, included funding for the Office of the Privacy Commissioner (OPC) to provide advice and conduct privacy audits to assist the three agencies (including DIAC) in addressing privacy issues that may arise because of the use of biometrics.[184]

4.35 To date, the OPC has conducted one information privacy principles audit in DIAC. The audit, conducted between November 2005-November 2006, focused on the design of DIAC's Identity Services Repository (ISR). The auditors concluded that:

> The systems design and specifications outlined by DIMA suggest that the ISR will provide an environment that generally supports the handling of personal information in accordance with the IPPs in the Privacy Act.[185]

[181] Photographs or fingerprints.

[182] A template or algorithm.

[183] *Migration Act 1958* (Section 333K (4)) and *Australian Citizenship Act 1997* (Section 45 (4)).

[184] Amanda Vanstone, 10 May 2005, Media Release: Development of Biometric Technology for Border Control—Joint Media Release with Ministers for Foreign Affairs and Justice and Customs.

[185] Office of the Privacy Commissioner, 2006, *Information Privacy Principles audit: Identity Services Repository (Systems Design)*, p. 6.

4.36 The OPC made ten recommendations to ensure that best practice privacy controls are built into the ISR. DIAC accepted seven of the recommendations. DIAC advised that the Identity Branch's newly created Governance, Evaluation and Monitoring (GEM) section (see paragraph 3.23) will be monitoring the implementation and impact of OPC's recommendations.[186]

4.37 Overall, the ANAO considers that DIAC needs to strengthen substantially its processes for assuring itself that the legislative requirements in relation to access, disclosure, retention and destruction of personal identifiers and related information are being implemented consistently and appropriately. In addition, the provisions in relation to retaining and destroying identifying information should be specifically examined in the scheduled review of the legislation (see paragraph 2.57) to ensure they are fully functional.

IT systems development

4.38 There are benefits to an organisation using system development methods and processes.[187] The appropriate use of a system development method should result in the delivery of a high quality system that meets or exceeds business expectations, within time and cost estimates, works effectively and efficiently in the current and planned information technology infrastructure, and is cost-effective to maintain and to modify.

4.39 The ANAO assessed[188] whether DIAC's biometric related IT projects:

- were supported by an effective system development framework;
- were effectively and appropriately applying aspects of DIAC's system development framework; and
- had implemented effective requirements management processes.

DIAC's systems development approach

4.40 When the biometric related IT initiatives commenced, DIAC did not have a formally documented system development methodology. However, as part of its SfP program DIAC has since established a Software Development

[186] GEM section is also tasked with monitoring the implementation of other review recommendations.

[187] IT Governance Institute, 2007, *Control Objectives for Information and Related Technology (CobiT)*, Version 4.1. Systems development methodologies can be either custom- or vendor-developed.

[188] The audit had regard to a number of better practice sources including the IT auditing standard known as Control Objectives for Information and Related Technology (CobiT).

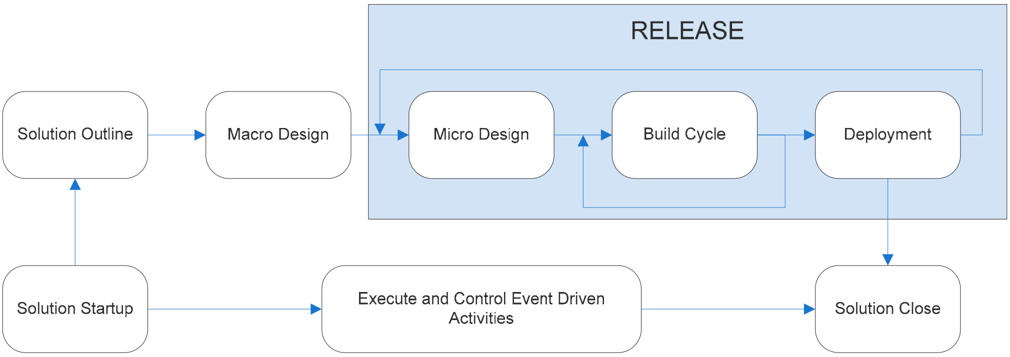
Life-cycle (SDLC) project[189] that aims to implement new system development policy, standards, guidelines, methods and tools appropriate to the DIAC environment. The SfP program selected IBM as its strategic technology partner, providing method and tool suites which are being adapted for DIAC use.

4.41 The SDLC project is currently in progress, and the systems development methodology is undergoing cycles of adaptation and implementation. Consequently, the ANAO considers the processes currently in place to have been defined but relatively immature in implementation.[190]

4.42 Figure 4.1 describes DIAC's IT system development lifecycle.

Figure 4.1

DIAC IT System Development Lifecycle



Source: ANAO, based on DIAC documentation.

4.43 DIAC has also implemented a new release management strategy in order to support the SfP program. All IT projects undertaking system development initiatives are to adhere to this release management strategy. The ANAO assessed whether DIAC's ISR and DCR biometric projects were following the new system development and release management processes.

Identity Services Repository (ISR) project

4.44 DIAC developed the ISR system in-house. The ANAO found that the project was following the new DIAC system development and release management process.

[189] The SDLC project commenced in September 2006.

[190] IT Governance Institute, 2007, *Control Objectives for Information and Related Technology (CobiT)*, Version 4.1.

Detention Centre Rollout (DCR) project

4.45 A contractor is working in partnership with DIAC on the DCR project. The DIAC Biometric Deed of Agreement governs the supply of biometric products and services to DIAC.[191]

4.46 At the time of contract negotiations, DIAC did not have a standard system development methodology, and instead used the methodology employed by the contractor.[192] However, the DCR project team is constrained by and must adhere to the new DIAC system development methodology (in the process of being implemented as part of the SfP program) and the new release management process. The ANAO found that the DCR project has implemented the new processes.

4.47 In any system development initiative, a number of system development 'artefacts', such as requirements, design, architecture, and testing specifications, are produced. The system development artefacts are important in providing each stakeholder with the information necessary for them to undertake their particular tasks. Failure to produce these artefacts increases the risk of wasted time and effort, arising from staff having incomplete information at the commencement of their work.

4.48 The ANAO observed that the DCR system development artefact documents were not formally reviewed and approved by all business stakeholders and groups involved in developing this system.

4.49 The ANAO considers that a formal process whereby DCR system development artefact documents are reviewed and approved by business stakeholders and groups involved in developing this system would strengthen quality assurance of system development artefacts.

Requirements management

Biometric project approach to requirements management

4.50 Requirements management involves establishing mechanisms to capture and track changes, and approvals for changes, to project requirements over the life of a system development project.[193] The ANAO assessed the requirements management processes implemented by the ISR and DCR projects.

[191] Associated work orders define the scope, roles, responsibilities, deliverables and costs for each element of work undertaken by the contractor.

[192] This was agreed upon in negotiations between DIAC and the contractor.

[193] Project requirements should include all rejected requirements.

4.51 The ANAO found that the ISR and DCR business requirement artefacts produced within each project's lifecycle indicate that requirements for the systems under development have been significantly modified over time, reflecting developments in DIAC's knowledge, technological advancements, and external factors such as government requirements.

4.52 The ANAO also found that, notwithstanding DIAC policy (see paragraph 3.44), DIAC did not have a requirements management mechanism for its ISR and DCR projects. Specifically:

- DIAC was not recording vital information such as: original requirements and their originator, changes applied to requirements and reasons for changes, changes to project scope including a determination of which requirements are to be delivered in which project stage, and evidence of approval of changes by business stakeholders and the systems development team ; and
- DIAC was not able to provide evidence that the design phase and subsequent design specifications captured all requirements specified in the analysis phase, nor that such requirements remained in scope for actual construction within the system and subsequent implementation.

4.53 The absence of an effectively implemented requirements management mechanism for biometrics projects raises risks that DIAC's biometric related system will be completed with only a percentage of originally specified features and functions, or that the features and functions implemented do not meet the needs of the business stakeholders.[194]

4.54 The ANAO found evidence of these risks eventuating. For example, the Identity Resolution Centre (IRC), a key DIAC business stakeholder in the development of the biometric solution,[195] conducted an initial phase of User Acceptance Testing of the biometric solution. IRC documentation from August 2007 indicated that the system did not meet the original stated requirements of the IRC, and '…*will require significant external system workarounds for functionality specific to IRC processes*'.[196]

[194] Consequential risks include: the system will not be accepted by the business stakeholders; compensating manual processes may need to be introduced (which will have associated costs, risks and inefficiencies); and further system re-development effort will be needed at an additional cost to address shortcomings in features and functions of the system.

[195] The biometric solution is scheduled for delivery as part of stage two of the DCR project.

[196] DIAC, 2007, *User Acceptance Testing Signoff project artefact for stage 2*, p. 6.

4.55 Overall, the ANAO considers that DIAC had generally adequate IT systems development for the introduction of biometrics. However, implementing an effective requirements management mechanism would assist DIAC in capturing and managing system features and functions that are required to meet the needs of business stakeholders. DIAC could strengthen its requirements management process by:

- undertaking a review of business requirements to identify those requirements which have been delivered to date within system implementations, those requirements that are still required and the associated priority, and those requirements that have been cancelled or deferred;
- implementing formal requirements management processes, to ensure that requirements are effectively captured and that changes to requirements are managed throughout the life of the project; and
- implementing a mechanism (such as requirements traceability matrix) which enables the tracing of business requirements through the general system development phases of analysis, design, construction, testing and implementation.

Conclusion

4.56 DIAC has prepared detailed draft guidance and adequate training on client identity matters, including biometrics. Although the guidance is sound its finalisation has not been timely. There have also been delays in up-loading the completed guidance onto LEGEND (the system through which DIAC staff can access policy guidance).

4.57 When the guidance is completed and is made available for staff, it would benefit from being accompanied by a performance monitoring and feedback strategy. DIAC's national Quality Assurance Framework may provide a suitable platform for obtaining this assurance.

4.58 DIAC has also prepared an Identity Management Training Plan 2007—2010, that maps out sound training initiatives for the Identity Branch.

4.59 In order to assure information privacy, DIAC designed its ISR so that access is based on a person's 'position number'. However, DIAC was unable to provide evidence of actions taken to ensure that access to identifying information was only by authorised officers. Further, there was no monitoring process to provide assurance about the appropriateness of access to identifying information by authorised officers.

4.60 Protections in the *Migration Act 1958* surrounding access to, and disclosure of, identifying information do not extend to third parties to which DIAC discloses information. DIAC cannot ensure that there is/will be no inappropriate use or disclosure of identifying information by the agencies to which it discloses the information. Stronger provisions in DIAC's Memoranda of Understanding would provide some further assurance that identifying information disclosed by DIAC to third parties is appropriately protected. There is also no effective process to provide assurance that disclosures of identifying information by DIAC officers are appropriately documented.

4.61 While there is a general legislative requirement to destroy identifying information, there are exceptions. These exceptions mean that DIAC is authorised to retain indefinitely virtually all of the biometric information it is currently planning to collect.[197]

4.62 DIAC's current Records Disposal Authority (RDA) provides for the disposal of records one year after 'the action is completed'. DIAC advised that it was 'looking at ensuring that dates of entry of data are flagged'. Although this will be a useful first step, DIAC needs to institute monitoring processes to identify aged information for destruction and should consider whether the legislative provisions with respect to the retention and destruction of identifying information are functioning fully as intended.

4.63 DIAC is in the process of implementing an IT system development framework that can support DIAC's current and future biometric software development activities. However, given the relative immaturity of the framework and tools, the ANAO was not in a position to assess its implementation.

4.64 As required by the Systems for People program, software development and release management process have been implemented for two of DIAC's biometric system development projects that are currently underway, the ISR and DCR projects.

4.65 However, for the DCR project, system development documents were not being formally reviewed or approved by all business stakeholders and

[197] Information such as biometric photographs from a range of visa and citizenship applicants, as well as fingerprints of people in immigration detention.

groups involved in developing the system. This is essential for quality assurance.

4.66 DIAC has not implemented its requirements management mechanism for its biometrics related IT projects. The absence of an effectively implemented requirements management mechanism raises risks that DIAC's biometric related system will be completed without all the originally specified features and functions, or that the features and functions implemented may not meet the needs of business stakeholders.[198] The ANAO found evidence of these risks eventuating.

Recommendation No.3

4.67 The ANAO recommends that, consistent with the direction taken in its National Quality Assurance Framework, DIAC:

- obtains structured feedback from decision makers on the usefulness of operational policy guidance relating to biometrics, and develops a means for obtaining assurance that decision makers are implementing the policy guidance consistently and appropriately; and
- strengthens its processes for obtaining assurance that the legislative requirements in relation to access, disclosure, retention and destruction of personal identifiers and related information are implemented consistently and appropriately.

DIAC response

4.68 Agree. DIAC agrees that obtaining structured feedback is important and is considering how this can best be achieved; taking into account that feedback from decision-makers will also be sought as part of the evaluation of the identity management strategy. DIAC has already commenced analysis of the current assurance processes surrounding the Identity Services Repository and has identified a number of potential refinements to the controls.

[198] Consequential risks include: the system may not be accepted by the business stakeholders; compensating manual processes may need to be introduced (which will have associated costs, risks and inefficiencies); and further system re-development effort may be needed at an additional cost to address shortcomings in features and functions of the system.

Recommendation No.4

4.69 The ANAO recommends that, in order to strengthen quality assurance for the development of IT systems, DIAC ensures that system development documents are reviewed and approved by business stakeholders and groups involved in developing these systems, and its requirements management mechanism is implemented for biometrics projects.

DIAC response

4.70 Agree. In 2006 DIAC introduced a new requirements management policy that is included in the overall departmental project management framework and is being used for all IT projects. In response to the ANAO comments, a requirements manager has been appointed specifically for the biometric projects.

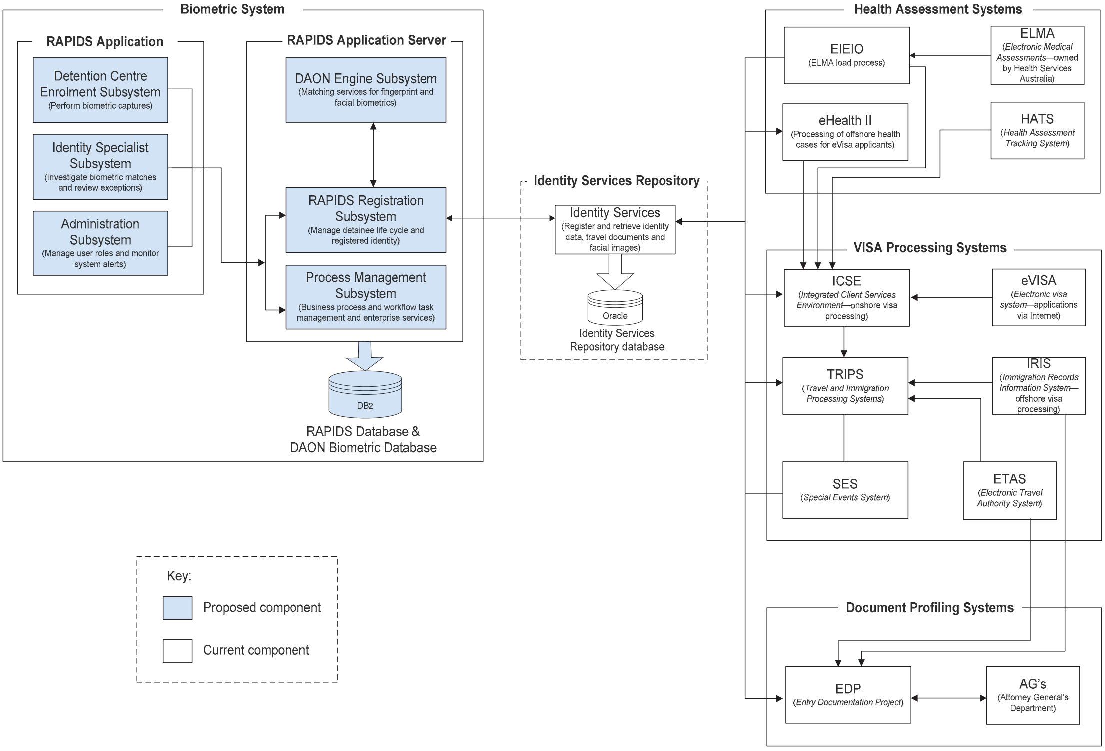
Ian McPhee
Auditor-General

Canberra ACT
26 February 2008

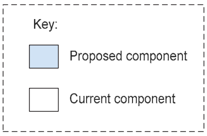
Appendices

Appendix 1: ISR System Interfaces—June 2007

The ISR connects to DIAC business applications such as: the Integrated Client Services Environment (ICSE);[199] Travel and Immigration Processing System (TRIPS);[200] the Entry Documentation Project (EDP);[201] and a number of health assessment systems.



Biometric System
RAPIDS Application
Detention Centre Enrolment Subsystem
(Perform biometric captures)
Identity Specialist Subsystem
(Investigate biometric matches and review exceptions)
Administration Subsystem
(Manage user roles and monitor system alerts)
RAPIDS Application Server
DAON Engine Subsystem
(Matching services for fingerprint and facial biometrics)
RAPIDS Registration Subsystem
(Manage detainee life cycle and registered identity)
Process Management Subsystem
(Business process and workflow task management and enterprise services)
DB2
RAPIDS Database & DAON Biometric Database
Identity Services Repository
Identity Services
(Register and retrieve identity data, travel documents and facial images)
Oracle
Identity Services Repository database
Health Assessment Systems
EIEIO
(ELMA load process)
ELMA
(Electronic Medical Assessments—owned by Health Services Australia)
eHealth II
(Processing of offshore health cases for eVisa applicants)
HATS
(Health Assessment Tracking System)
VISA Processing Systems
ICSE
(Integrated Client Services Environment—onshore visa processing)
eVISA
(Electronic visa system—applications via Internet)
TRIPS
(Travel and Immigration Processing Systems)
IRIS
(Immigration Records Information System—offshore visa processing)
SES
(Special Events System)
ETAS
(Electronic Travel Authority System)
Document Profiling Systems
EDP
(Entry Documentation Project)
AG's
(Attorney General's Department)



Source: ANAO, derived from DIAC documents.

Note: Not all interfaces between business systems have been represented in this diagram.

[199] ICSE maintains information regarding client requests for citizenship, onshore and offshore visa grants.

[200] TRIPS manage border clearance processing and hold the database of record of Australian visas, traveller movements, Australian and New Zealand passports and the Movement Alert List. The system facilitates the processing of travellers moving through immigration clearance points at Australia's border.

[201] DIAC's document profiling system.

Appendix 2: Client-side and Server-side Subsystems of DIAC's Proposed Biometric Solution

Proposed DCR Project Biometric Solution—Client Subsystems

Subsystem	Purpose
DCR Enrolment	To enable biometric capture and enrolment. To be used by the detention services contract provider.
Identity Specialist	To provide 'Investigate', 'Biometric Match' and 'Review Exception' functions. To be used by DIAC officers.
Administration	To provide functions to manage users, roles and monitor for system alerts which will be deployed on designated administrator workstations. To be used by DIAC officers.

Source: DIAC Detention Centre Rollout Updated Solution Architecture Version 5.0 June 2007

Proposed DCR Project Biometric Solution—Server Subsystems

Subsystem	Purpose
RAPIDS Process Management	To orchestrate the business process flows, workflow task management, and enterprise services such as auditing.
RAPIDS Registration	To manage the life-cycle of the detainee and the registered identity, and will act as a hub to ISR and DAON services.
DAONEngine	To provide the matching services for Fingerprint and Facial biometrics.

Source: DIAC Detention Centre Rollout Updated Solution Architecture Version 5.0 June 2007

Appendix 3: Defence Science and Technology Organisation Reports into the Effects Associated with Biometric Enrolment and Verification on DIAC

- DSTO-GD-0476, October 2006, *Analysis into the Effects Associated with Biometric Enrolment and Verification on Department of Immigration and Multicultural Affairs Business Practices–Summary of the Operational Based Analyses Resulting from Biometric Trials in Australia and Overseas (April 2005 to March 2006)*.
- DSTO-TR-1913, November 2006, *Analysis into the Effects Associated with Biometric Enrolment and Verification on Department of Immigration and Multicultural Affairs Business Practices–Overall Performance of the Operational Based Analyses Resulting from Biometric Trials in Australia and Overseas (April 2005 to March 2006).*
- DSTO-TR-1869, June 2006, *Operational Analysis into the Effects Associated with Biometric Enrolment on Department of Immigration and Multicultural Affairs Business Practices–First Operational Study (April to July 2005)*.
- DSTO-TR-1858, July 2006, *Operational Analysis into the Effects Associated with Biometric Enrolment and Verification on Department of Immigration and Multicultural Affairs Business Practices at Sydney Kingsford Smith Airport (August to December 2005)*.
- DSTO-TR-1878, July 2006, *Operational Analysis into the Effects Associated with Biometric Enrolment and Verification on Department of Immigration and Multicultural Affairs Business Practices in an Overseas Environment–Mobile Team Visit 1 (August to September 2005)*.
- DSTO-TR-1877, July 2006, *Operational Analysis into the Effects Associated with Biometric Enrolment and Verification on Department of Immigration and Multicultural Affairs Business Practices in an Overseas Environment–Mobile Team Visit 2 (January to March 2006)*.

Source: DIAC.

Appendix 4: Timeline of Expected Deliverables January 2007 to June 2009

Timeframe	Expected deliverable	IP 2006–07	IP 2007–08	SP 2007
Jan-Mar 07				
Apr-Jun 07	Investigate the accessing of biometric data enabling agencies to collect, store and use biometric images to support its own and other agency's identity management responsibilities – Business options for data access with NZ and DFAT	√		
	Plan the further integration of the Customs border processing and DIMA identity mgt systems to expand the use of biometric technology in the non-citizen caseload and to deliver an integrated solution at the primary line – Feasibility study	√		√
	Revised MSIs to support new & enhanced business processes			√
	Business rules to support enhanced client identity search			√
	Training plans to support new identity management capability			√
	Standards to support image capture of face, finger scan and document images			√
Jul-Sep 07	Effective program management, monitoring and reporting - v 3 of the Implementation Plan	√		
	Plan the further integration of the Customs border processing and DIMA identity mgt systems to expand the use of biometric technology in the non-citizen caseload and to deliver an integrated solution at the primary line – Business case	√	√	
	The phased application of Biometric Technology for identity mgt and border control services to enable better identification and screening of non-citizens, including possibly high-risk or undesirable individuals seeking to enter Australia – Biometric enrolment & matching enabled with ISR	√		
	Organisational change management plan for identity management		√	√
	Communications plan for identity management strategy		√	√
	Training plan and strategy for single client view, identity resolution, citizenship testing and DVS		√	√
	New procedures and regulations for identity resolution processes		√	√
	Business rules for advanced data matching		√	√

Timeframe	Expected deliverable	IP 2006–07	IP 2007–08	SP 2007
	Business rules defined for one-one and one-many finger scan and facial matching		√ (Technical capability)	√
	Report providing cost estimates and business process change required to implement new NISS standards for Proof of Identity docs		√	√
	Report providing cost estimates and business process changes reqd to implement biometric data collection and sharing between Customs and DIAC		√	√
	Joint NPP between DIAC and Customs for implementing the recommended biometric solution for data collection and sharing		√	√
	Initial identity risk model		√	√
Oct-Dec 07	Investigate the accessing of biometric data enabling agencies to collect, store and use biometric images to support its own and other agency's identity management responsibilities- Technical options for data access with NZ and DFAT	√		
	Plan the further integration of the Customs border processing and DIMA identity mgt systems to expand the use of biometric technology in the non-citizen caseload and to deliver an integrated solution at the primary line – NPP for integration of the Customs border processing and DIMA identity mgt systems	√	√	
	The phased application of Biometric Technology for identity mgt and border control services to enable better identification and screening of non-citizens, including possibly high-risk or undesirable individuals seeking to enter Australia -	√	√	
	(a) Pilot biometric matching with alert systems	√		
	(b) Identity mgt using biometrics enabled for Ref&Hum PV caseload	√	√	
	Training plans and strategy for integrated visa processing, client self service, case mgt, identity resolution capability		√	√
	New procedures and regulations for escalation of identity resolution including business rules for automated escalation of client self service cases		√	√
	New procedures to support enhanced document examination		√	√
	New processes to support fraud recording, reporting and monitoring		√	√
	Enhancements to the identity risk model		√	√

Timeframe	Expected deliverable	IP 2006–07	IP 2007–08	SP 2007
	Business options for biometric data sharing with DFAT and NZ completed		√	√
Jan-Mar 08	Plan the further integration of the Customs border processing and DIMA identity mgt systems to expand the use of biometric technology in the non-citizen caseload and to deliver an integrated solution at the primary line – Budget decision	√	√	
	The phased application of Biometric Technology for identity mgt and border control services to enable better identification and screening of non-citizens, including possibly high-risk or undesirable individuals seeking to enter Australia – Roll out of biometric matching with alert systems	√		
	Training plans and strategy for new capability- level of confidence and DVS		√	√
	New procedures for incorporating level of confidence into visa processing and identity resolution		√	√
	New procedures to support DVS processes		√	√
	New procedures to support pilot biometric watch list		Deferred	√
Apr-Jun 08	Investigate the accessing of biometric data enabling agencies to collect, store and use biometric images to support its own and other agency's identity management responsibilities- Feasibility report on data access with NZ and DFAT.	√	√ (Technical options for data access w/ NZ & DFAT)	
	The phased application of Biometric Technology for identity mgt and border control services to enable better identification and screening of non-citizens, including possibly high-risk or undesirable individuals seeking to enter Australia – Biometric alert systems linked to Crimtrac	√	√	
	Training plans and strategy for new capability – capturing of finger scans in Refugee & Humanitarian and onshore protection and use of relevant components of the identity mgt suite in integrated visa processing (VS05, CSS05 case loads), contact ctr (CC02), case mgt (CM04) and detention processing (DS02)		√	√
	New procedures and regulations for use of 3rd parties or other govt agencies to collect identity information at selected offshore posts		√	√
	New procedures for escalating identity resolution in VS05, CSS05, refugee and humanitarian, offshore processing, contact ctr (CC02), case mgt (CM04) and detention processing (DS02)		√	√
	Business specification of reporting reqts and follow-on processes			√

Timeframe	Expected deliverable	IP 2006–07	IP 2007–08	SP 2007
	Updates to identity mgt related standards (face, finger scan, POI docs and any others reqd)		√	√
	Feasibility report on incorporating matchng biographical data against external commercially available data holdings into identity mgt suite		√	√
	Report on outcome of biometric watch list pilot		√	√
Jul-Sep 08	Effective program management, monitoring and reporting - v 4 of the Implementation Plan	√		
	Training plans and strategy for new capability-use of relevant components of the identity mgt suite in integrated visa processing (VS06 and CSS06 case loads)			√
	New procedures for escalating identity resolution in VS06, CSS06 processing			√
	New procedures for use of identity mgt suite in VS06, CSS06 processing			√
	New procedures to support fully operational biometric watch list			√
	New procedures for use of identity mgt suite for external stakeholders/partners			√
	Business specification of reporting reqts and follow-on processes			√
Oct-Dec 08	Training plans and strategy for new capability-use of relevant components of the identity management suite in integrated visa processing (VS07 and CSS07 case loads) and settlement services (SS02) and use of new DIAC POI documents			√
	New procedures for escalating identity resolution in VS07, CSS07, SS02 processing			√
	New procedures for use of relevant components in the identity mgt suite in VS07, CSS07, SS02 processing			√
	Business specification of reporting requirements and follow-on processes			√
	DIAC POI documents with enhanced security features are available and in use (DFFTA, Citizenship, PL056)			√
Jan-Mar 09	The phased application of Biometric technology for identity mgt and border control services to enable better identification and screening of non-citizens, including possibly high-risk or undesirable individuals seeking to enter Australia – Identity mgt using biometrics enabled at airports	√		
	Training plans and strategy for new capability-use of relevant components of the identity mgt suite in integrated visa processing (VS08 and CSS08 case loads) and stakeholder/partners			√

Timeframe	Expected deliverable	IP 2006–07	IP 2007–08	SP 2007
	New procedures for escalating identity resolution in VS08, CSS08, SP03 processing			√
	New procedures and regulations for use of relevant components of the identity mgt suite in VS08, CSS08, SP03 processing			√
	Business specification of reporting reqts and follow-on processes			√
Apr-Jun 09	The phased application of Biometric technology for identity mgt and border control services to enable better identification and screening of non-citizens, including possibly high-risk or undesirable individuals seeking to enter Australia – Identity management using biometrics enabled at the border	√		
	Training plans and strategy for new capability-use of relevant components of the identity mgt suite in border processing (BS03) and settlement processing (SS03).			√
	New procedures for escalating identity resolution in BS03 and SS03 processing			√
	New procedures for use of identity mgt suite in BS03 and SS03 processing			√
	Business specification of reporting requirements and follow-on processes			√

Source: ANAO analysis using DIAC documents.

Note: √ - the deliverable exists under the particular plan.

The expected deliverables under the Implementation Plans (IPs) cover general business and IT deliverables. The items under the Strategic Plan (SP) cover business deliverables only.

Appendix 5: Purpose of Personal Identifiers in the *Migration Act 1958*

Section 5A

…

(3) The purposes are:

(a) to assist in the identification of, and to authenticate the identity of, any person who can be required under this Act to provide a personal identifier; and

(b) to assist in identifying, in the future, any such person; and

(c) to improve the integrity of entry programs, including passenger processing at Australia's border; and

(d) to facilitate a visa holder's access to his or her rights under this Act or the regulations; and

(e) to improve the procedures for determining visa applications; and

(f) to improve the procedures for determining claims for protection under the Refugees Convention as amended by the Refugees Protocol; and

(g) to enhance the Department's ability to identify non citizens who have a criminal history, who are of character concern or who are of national security concern; and

(h) to combat document and identity fraud in immigration matters; and

(i) to detect forum shopping by applicants for visas; and

(j) to ascertain whether:

(i) an applicant for a protection visa; or

(ii) an offshore entry person who makes a claim for protection under the Refugees Convention as amended by the Refugees Protocol;

had sufficient opportunity to avail himself or herself of protection before arriving in Australia; and

(k) to complement anti people smuggling measures; and

(l) to inform the governments of foreign countries of the identity of non citizens who are, or are to be, removed or deported from Australia.

Index

Series Titles

Audit Report No.1 2007–08
Acquisition of the ABRAMS Main Battle Tank
Department of Defence
Defence Materiel Organisation

Audit Report No.2 2007–08
Electronic Travel Authority Follow-up Audit
Department of Immigration and Citizenship

Audit Report No.3 2007–08
Australian Technical Colleges Programme
Department of Education, Science and Training

Audit Report No.4 2007–08
Container Examination Facilities Follow-up
Australian Customs Service

Audit Report No.5 2007–08
National Cervical Screening Program Follow-up
Department of Health and Ageing

Audit Report No.6 2007–08
Australia's Preparedness for a Human Influenza Pandemic
Department of Health and Ageing
Department of Agriculture, Fisheries and Forestry

Audit Report No.7 2007–08
The Senate Order for Departmental and Agency Contracts (Calendar Year 2006 Compliance)

Audit Report No.8 2007–08
Proof of Identity for Accessing Centrelink Payments
Centrelink
Department of Human Services

Audit Report No.9 2007–08
Australian Apprenticeships
Department of Education, Science Training

Audit Report No.10 2007–08
Whole of Government Indigenous Service Delivery Arrangements

Audit Report No.11 2007–08
Management of the FFG Capability Upgrade
Department of Defence
Defence Materiel Organisation

Audit Report No.12 2007–08
Administration of High Risk Income Tax Refunds in the Individuals and Micro Enterprises Market Segments
Australian Taxation Office

Audit Report No.13 2007–08
The Australian Taxation Office's Approach to Managing Self Managed Superannuation Fund Compliance Risks
Australian Taxation Office

Audit Report No.14 2007–08
Performance Audit of the Regional Partnerships Programme:
Volume 1–Summary and Recommendations
Volume 2–Main Report
Volume 3–Project Case Studies
Department of Transport and Regional Services

Audit Report No.15 2007–08
Administration of Australian Business Number Registrations: Follow-up Audit
Australian Taxation Office

Audit Report No.16 2007–08
Data Integrity in the Child Support Agency
Child Support Agency
Department of Human Services

Audit Report No.17 2007–08
Management of the IT Refresh Programme
Centrelink

Audit Report No.18 2007-08
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2007

Audit Report No.19 2007–08
Administration of the Automotive Competitiveness and Investment Scheme
Department of Innovation, Industry, Science and Research
Australian Customs Service

Audit Report No.20 2007–08
Accuracy of Medicare Claims Processing
Medicare Australia

Audit Report No.21 2007–08
Regional Delivery Model for the Natural Heritage Trust and the National Action Plan for Salinity and Water Quality
Department of the Environment, Water, Heritage and the Arts
Department of Agriculture, Fisheries and Forestry

Audit Report No.22 2007–08
Administration of Grants to the Australian Rail Track Corporation
Department of Infrastructure, Transport, Regional Development and Local Government

Audit Report No.23 2007–08
The Management of Cost Recovery by Selected Regulators

Current Better Practice Guides

The following Better Practice Guides are available on the Australian National Audit Office Website.

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
Legal Services Arrangements in Australian Government Agencies	Aug 2006
Preparation of Financial Statements by Public Sector Entities	Apr 2006
Administration of Fringe Benefits Tax	Feb 2006
User–Friendly Forms	
Key Principles and Practices to Effectively Design and Communicate Australian Government Forms	Jan 2006
Public Sector Audit Committees	Feb 2005
Fraud Control in Australian Government Agencies	Aug 2004
Security and Control Update for SAP R/3	June 2004
Better Practice in Annual Performance Reporting	Apr 2004
Management of Scientific Research and Development Projects in Commonwealth Agencies	Dec 2003
Public Sector Governance	July 2003
Goods and Services Tax (GST) Administration	May 2003
Managing Parliamentary Workflow	Apr 2003
Building Capability—A framework for managing learning and development in the APS	Apr 2003
Internal Budgeting	Feb 2003
Administration of Grants	May 2002
Performance Information in Portfolio Budget Statements	May 2002

Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	June 2001
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Commonwealth Agency Energy Management	June 1999
Security and Control for SAP R/3	Oct 1998
Controlling Performance and Outcomes	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997