The Auditor-General
Audit Report No.35 2008–09
Performance Audit

Management of the Movement Alert List

Department of Immigration and Citizenship

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 81067 2

Australian National
Audit Office

Canberra ACT
21 May 2009

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 *Management of the Movement Alert List.*

Following its tabling in Parliament, 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 (ANAO). 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 Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Telephone: **(02) 6203 7505**
Fax: **(02) 6203 7519**
Email: **webmaster@anao.gov.au**

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

http://www.anao.gov.au

Audit Team
David Rowlands
Jason McKenzie
Tom Clarke

Contents

Tables

Figures

Abbreviations/Glossary

Alert Reason	A reason for entering a record of a person on MAL (see ARC).
ALO	Airline Liaison Officer, a DIAC officer stationed at certain international airports to help with problems arising from travellers' documentation.
ARC	Alert Reason Code. A code representing a category of reason for placing a record on MAL. A list of Alert Reasons is set out at Appendix 1.
ASIO	The Australian Security Intelligence Organisation, Australia's national security service.
BOC	Border Operations Centre. A combination of the Entry Operations Centre (cf. EOC) and Central MAL Operations Section in DIAC's national office, Canberra.
CMAL	Central MAL. This is the redeveloped MAL, based on a new applications system and mode of operation where all the possible matches identified by the system are resolved centrally in DIAC's Border Operations Centre, in Canberra (see Chapter 9). Note that 'CMAL' refers to both the system and the database.
DAL	Document Alert List. One of two subsidiary databases that comprise MAL (see also PAL).
DIAC	Department of Immigration and Citizenship
EOC	Entry Operations Centre. A unit in DIAC's National Office, which helps with problems arising with travel documentation and so on at airports and the border (cf. BOC).
Health Undertaking	A visa applicant can attract a health undertaking with a medical condition that requires follow up treatment or examination once they are in Australia.
HMAL	Heritage MAL. A term used by DIAC to refer to the older MAL system, to distinguish it from, and which is replaced by, CMAL.
MAL	Movement Alert List. 'MAL' (now known as 'CMAL') is the name of both the application system and the database. Generally, references in this report to MAL are to the database.
MDS	Minimum Data Standards. The minimum acceptable set of information for an entry in MAL.
MOU	Memorandum of Understanding

PACE	Passenger Analysis, Clearance and Evaluation system. An Australian Customs and Border Protection Service computer system used at Australia’s borders.
PAL	Person Alert List. One of two subsidiary databases that comprise MAL (see also DAL).
PAM3 manual	DIAC’s Policy Advice Manual, containing comprehensive policy and procedural advice to DIAC officers.
RIF	Remote Input Function. A facility for entering data into MAL.
SRS	Security Referral Service. A new system to facilitate communications between DIAC and ASIO to support security checking of those who seek to travel to Australia.
STOs	State and Territory Offices (of DIAC)

Summary and Recommendations

Summary

Introduction

1. The Movement Alert List (MAL) is a computer database maintained by the Department of Immigration and Citizenship (DIAC) to protect the country from those people who may pose a threat to the Australian community. MAL is used to inform decisions about visa and citizenship grant and admission of non-citizens into the country. Checking takes place at several points, contributing to a 'layered' approach to border management. In this way, MAL forms an important element in Australia's national security and border protection strategy.

2. MAL contains two subsidiary databases: the first, the Person Alert List (PAL), contains adverse information about people who are placed on this list for various reasons ('Alert Reasons'). The second is the Document Alert List (DAL), primarily a list of lost and stolen travel documents. DIAC checks MAL when any non-citizen seeks a visa, seeks to travel to or enter Australia or applies for citizenship. Essentially, MAL is a collection of information about identities and travel documents of interest, primarily, to visa decision-makers.

3. Travel to and from Australia has continued to grow in recent years[1] and the number of records in MAL has also grown in complexity and size, particularly after 2001. It now has around 680 000 PAL and over two million DAL records. Over half of PAL comprises records of non-citizens of national security concern.

4. The growth of the number of records in MAL has been encouraged by DIAC so as to maximise the likelihood of identifying a non-citizen of concern travelling, or seeking to travel, to Australia. Under such an approach it is important that the department have in place appropriate arrangements to review the quality of records over time to avoid deterioration in the quality of the database and the matches it generates.

5. The 2003 Budget funded a proposal to have a task force review MAL (the Wheen Review). Subsequently, DIAC obtained government approval and funding in the 2005 Budget to implement the recommendations of the Review.

[1] Any changes in trend that may flow from the global financial crisis that commenced in late 2008 are not reflected in the available data, which covers the period to the end of the financial year 2007–08.

Among other things, the Review identified risks in MAL's then mode of operation and proposed redevelopment of the system with all MAL checking taking place centrally. This has been the CMAL project, which was being implemented at the time of the audit.

Audit objectives and scope

6. The objective of the audit was to assess the effectiveness of DIAC's management of MAL. The scope was confined to DIAC's management and use of the system: it did not examine the work of others with an interest in the system, such as security agencies.

Overall conclusion

7. Successive reviews over more than a decade have judged MAL to be conceptually sound and an increasingly important part of the suite of facilities used by DIAC and related agencies to control entry to Australia. MAL provides important information to DIAC decision-makers to help in deciding visa and citizenship applications and whether a person should be allowed into Australia.

8. DIAC has managed an extended period of growth in the numbers of records in MAL by adding substantial numbers of *National Security* records and maintaining light controls on new entries provided by departmental staff. However, the department has been less successful in ensuring the quality of its MAL records.

9. All the reviews of MAL have stressed the importance of it comprising sound data. However, the completeness, quality and currency of MAL data has proved an enduring problem for DIAC. Despite efforts to improve MAL data, the overall quality of data has been declining in recent years. Contributing to this position has been the challenge faced by the department in implementing an effective accountability regime to assure the quality of records over time.

10. Further, at an operational processing level, gaps have occurred in the arrangements designed to provide the department with assurance that all elements of MAL are working as intended. Given the centrality of the system to border protection, this aspect of the department's operations needs to be upgraded so that attention is drawn promptly to any substantial element that is not operating properly.

11. Over the last four years, DIAC has successfully managed the development and implementation of the new version of MAL, CMAL. This addresses certain substantial risks identified by the Wheen Review. The introduction of CMAL has improved management control over DIAC's MAL operations and provides a basis for DIAC to enhance its quality assurance of MAL data and of the operation of the system as a whole.

12. The ANAO has made five recommendations aimed at improving the effectiveness of DIAC's management of MAL.

Key findings by chapter

DIAC management of MAL data (Chapter 2)

13. Earlier reviews of MAL have identified persistent shortcomings in the management of MAL data: in collecting all the right records, in maintaining data quality and in deleting outdated information. Audit analysis showed that these shortcomings endure. This could lead to:

- failure to identify a person who poses a threat to the community if they are not on the list when DIAC checks and a consequent risk of admitting such a person;
- inefficient processing where information is incomplete or out-of-date;
- vigilance fatigue among MAL staff; and
- some loss of confidence in the MAL system as a whole.

14. Regardless of the particular data quality issue, DIAC needs to resolve who is responsible for the integrity of its MAL data. This is both a persistent and strategic issue. Currently, much depends on the soundness of the original data entry by any of several thousand staff. There is no substantial edit-checking at data entry to ensure the quality of the information that is entered.

15. Records are entered into MAL for any of a variety of 'Alert Reasons', reflecting the specific interests of DIAC 'Alert Reason owners' in diverse parts of the department and from external agencies. However, most DIAC Alert Reason owners, though regarded as 'data owners', have not assumed full responsibility for the data. This is because the data is and can be entered by many officers throughout DIAC and externally, action over which DIAC Alert Reason owners have no control.

16. DIAC is well aware of the deficiencies in its own MAL data. It has carried out regular reviews with the intention of identifying and, ultimately, correcting such deficiencies. Most often, these actions falter at the point where someone within DIAC has to take responsibility for carrying out corrective action. The issue of data ownership has long been identified but it clearly requires firm management decisions and action to address it.

17. Several streams of action are needed to deal with both the stock and the flow of data involving clarification of responsibilities, adoption of a strategy to ensure compliance of new entries with DIAC's business rules and an approach to reviewing existing data with a view to cleansing the database.

Controlling access to MAL (Chapter 3)

18. DIAC has a system in place to control who has access to MAL which, if it continues the active review process that it started in 2007, will allow it to maintain that control. Reviewing all MAL transactions would be resource-intensive but DIAC could address the lack of quality control over data entry by review of a risk-based sample of change/update transactions. These reviews could also be part of a generally improved system of quality control over MAL data entry.

Australian citizens on MAL (Chapter 4)

19. DIAC's policy on the inclusion of Australians on MAL is not currently coherent or complete. It has not fully clarified its reasons for wanting to list Australians on MAL nor, therefore, identified the specific characteristics that would justify considering Australians for listing on PAL. It would benefit from doing so and then confirming that there is a sound legal basis for each reason. It could then revise its PAM3 manual on this matter accordingly.

20. Although action has been recommended or begun several times to cull inappropriate records of Australian citizens, it has not been completed. Moreover, new such records are being entered.

21. The failure to cull records is attributed in DIAC's internal review of July 2005 to 'little priority being given to cleansing' PAL. A related question is the lack of clear responsibility for those records by various areas of DIAC—the question of data ownership. When policy has been clarified, its legal basis verified, and clear accountability has been set, DIAC will be in a position to more effectively cull inappropriate records of Australians on MAL.

Privacy and MAL (Chapter 5)

22. DIAC is aware of the importance of privacy of personal information and the relevant requirements of its own legislation and the Privacy Act. It is also aware that MAL very largely comprises personal information, some of which is sensitive. DIAC has not considered the privacy implications of its use of MAL in any substantial way. At one point, the department contemplated but did not proceed with a Privacy Impact Assessment (PIA) for MAL during its CMAL project. It is apparent from the analysis in Chapter 5 that DIAC would be better able to assure itself that it satisfies the Information Privacy Principles if it were to conduct a PIA of its administration of MAL. The department has agreed to do so.

MAL data-matching (Chapter 6)

23. Over the last decade DIAC has gradually extended sophisticated data-matching software to its visa processing and border operations systems. CMAL has enabled DIAC to address the main risks the department was formerly exposed to of not using its best data-matching software in each visa processing system and varying threshold scores. DIAC has recognised the need to continually tune and refine this software.

24. DIAC now has a strategy encompassing biographic (MAL) and biometric elements, acknowledging that identity management will become a more complex task in future.

MAL's interaction with migration law (Chapter 7)

25. The risk of DIAC granting a visa without first conducting a MAL check seems slight. However, DIAC regards performing MAL checks as an essential part of border protection. This suggests that DIAC should seek a remedy for its current inability to *require* delegates to check MAL. A remedy could take the form of the preparation of a new ministerial direction under s. 499 of the Migration Act. This would bring its current practice and its legal framework into harmony. DIAC has agreed to consider this course of action.

Assessing MAL's performance (Chapter 8)

26. On a number of occasions it has been apparent that DIAC has no information that shows how successful MAL is in helping it to achieve its outcomes. DIAC produces no data of this kind.

27. In administering a key business system, such as MAL, a balance should be struck between the cost of collecting performance information and the benefits to DIAC and key stakeholders, such as the Parliament, of this information in demonstrating MAL's successes. In this context, sound performance information would include data on DIAC's success in using MAL to (i) prevent people from entering Australia who pose a threat to the community and (ii) prevent such people from getting Australian citizenship. The range of other measures identified in the chapter could also help DIAC gauge the value being added by its use of MAL.

28. Management information on MAL is limited. It would help DIAC to manage MAL better if it were to measure and report internally on data quality, client service, and overall system reliability.

29. DIAC has suffered a number of failures in parts of MAL and each of these has remained undetected for an extended period. Although there is no evidence that any of these incidents has resulted in any inappropriate admissions into Australia, the department needs to have a mechanism in place that will draw such incidents to attention promptly in future.

CMAL implementation (Chapter 9)

30. DIAC has successfully introduced the CMAL system, which now operates in all visa processing systems. DIAC has pursued CMAL implementation as its most important priority in MAL operations, following the actual MAL-checking role itself. It has fulfilled the relevant project objectives set out in the CMAL Baseline Project Management Plan. Most important, the CMAL implementation has addressed two major risks by using DIAC's stronger name-matching software in all MAL-matching and having possible matches decided by experts in the Border Operations Centre.

31. CMAL implementation has taken two years longer than originally envisaged. During the project, DIAC's major Systems-for-People project introduced a new and different IT environment in which to progress, and this alone set the CMAL schedule back by about a year. However, despite the contingencies faced by the CMAL project over this time, DIAC has successfully managed its way through these and delivered its core undertakings.

32. Certain major tasks remain, such as decommissioning the old version of MAL, HMAL, and switching over wholly to the new system. Full realisation of benefits from the IT project will only be achieved after these changes have been implemented. Moreover, the original project encompassed measures agreed by the Government beyond the core IT redevelopment of MAL and centralising of MAL operations and which have not yet been implemented. These included the development of a reporting strategy and quality assurance process.

33. DIAC has not pursued its original proposals for measuring and reporting the performance of this project, though it did report progress of the core project through the CIU while required to do so. However, arrangements should be in place to give confidence that the decisions of government are effectively implemented; and when major changes are necessary, that the stakeholders are appropriately informed.

34. DIAC has advised that it intends to report to government, through the portfolio minister, once the CMAL NPP project wraps up at the end of 2008–09. It has undertaken to present a complete overview of the project in early 2009–10 which will include reporting against its original project objectives, as agreed by government in 2005. This includes each item specifically identified in the approved proposal.

Agency response

DIAC welcomes the audit of the management of the Movement Alert List, which has made a number of observations and recommendations that will assist the department in the ongoing effective and efficient management of the MAL system.

MAL is a complex system that has been in operation for many years, and has been subject to a number of reviews and refinements. It has served DIAC and Australia extremely well. It is a key component of the layered approach to border management and a critical contributor to national security. The ANAO report notes that successive reviews have judged MAL to be conceptually sound and an increasingly important part of the suite of facilities used to control entry to Australia. DIAC continues to improve the MAL system, and the successful introduction of the new Central MAL (CMAL) system has already addressed some of the matters raised in the audit report.

We note the areas for potential improvement that the report highlights in respect of data management, data quality and system monitoring. The recommendations in these areas are supported. Data quality issues also reflect the risk environment in which MAL has operated—in particular, with high growth in records over an extended period, reflecting heightened concerns about national security, fraud and irregular people movements.

We agree that there is room for greater efficiency in respect of data management and data quality and measures are being put in place to address this. The primary concern remains that MAL brings relevant and useful information to the attention of visa decision makers and key stakeholder agencies.

Recommendations

Set out below are the ANAO's recommendations aimed at strengthening management of the Movement Alert List. Report references and abbreviated agency responses are included. More detailed responses are in the body of the report.

Recommendation No. 1

Para. 2.143

The ANAO recommends that DIAC develop a plan for the population, maintenance and review of the MAL database. This should include, at a minimum:

- clarification as to who (within the department and externally, as appropriate) is responsible for MAL data, the quality issues to be addressed and business rules for addressing them; and
- a course of action which includes:
  - arrangements for data entry into MAL that ensures its own business rules and desired quality standards are observed;
  - instigation of a program, with target dates, for data cleansing its existing stock of MAL records; and
  - a mechanism for reviewing and reporting progress with this work.

DIAC response: *Agreed*

Recommendation No. 2

Para. 4.36

The ANAO recommends that DIAC:

- clarifies the circumstances in which it can properly record Australian citizens on MAL, consulting other agencies with an interest in MAL as appropriate;
- in this light, revises its policy and procedural guidelines for recording Australian citizens on MAL; and
- completes its review of records of Australians on MAL, and deletes records of Australians where they are inappropriately recorded.

DIAC response: *Agreed*

Recommendation No. 3

Para. 8.32

The ANAO recommends that DIAC improves its reporting on the performance of MAL by, where practicable, identifying instances where MAL has alerted its decision makers to information that has been the reason, or part of the reason, for decisions on visa and citizenship applications.

DIAC response: *Agreed*

Recommendation No. 4

Para. 8.69

To enable DIAC to manage MAL effectively, the ANAO recommends that DIAC seek to measure and report internally on:

(a) data quality;

(b) MAL's reliability; and

(c) client service, measured by the service level agreements agreed internally with CMAL client areas of the department.

DIAC response: *Agreed*

Recommendation No. 5

Para. 8.70

The ANAO recommends that DIAC implements a mechanism for providing regular assurance that all key parts of the MAL system are operating satisfactorily.

DIAC response: *Agreed*

Audit Findings and Conclusions

1. Introduction to MAL and this performance audit

This chapter explains what MAL is, what it does, why the ANAO has audited it and how we have done that.

MAL helps to protect the Australian community

1.1 The Movement Alert List (MAL) is a Department of Immigration and Citizenship (DIAC) computer database used by the Commonwealth to protect the country from those people who may pose a threat to the Australian community.[2] DIAC also uses it to avoid inappropriately conferring citizenship. The decision-maker grants, or refuses to grant, a visa or citizenship, or cancels a visa, based on all the relevant information available to them including any brought to their attention by MAL. MAL is also used at overseas check-in, while the vessel is in transit and at the border to clear people seeking to travel to and enter the country.

1.2 MAL is not a government program in itself but an administrative tool DIAC uses across many of its programs.[3] It comprises a repository of data linked to a matching and alert mechanism for decision-makers. The data comprises two lists: first, over 680 000 records of people for whom DIAC holds adverse information (the Person Alert List, 'PAL'); and second, 2.4 million records of travel documents believed to have been stolen or lost, or are suspected to be bogus (the Document Alert List, 'DAL').

1.3 When any non-citizen seeks an Australian visa, tries to travel to or enter Australia, or seeks citizenship, DIAC checks MAL for any information on that person or the travel document they present. DIAC uses software to help match the client details against MAL records. If it holds adverse information, this may lead to an adverse decision for the traveller or applicant. The action an official takes after getting a MAL alert depends on the circumstances including all the information they have before them. Being on MAL does not lead inevitably to an unfavourable result for the person listed.

[2] DIAC, <http://www.immi.gov.au/managing-australias-borders/border-security/systems/mal.htm> [accessed 7 May 2009].

[3] DIAC's immigration function makes greater use of MAL than does citizenship, and most relevant activities form part of DIAC Output 1.3.1, *Borders*, under Output Group 1.3, *Border Security*.

1.4 MAL has no specific basis in the law. However, it has become an essential tool to apply legislation governing the entry to and presence in Australia of persons who are of immigration, character and national security concern. In particular, it helps to identify people who may not satisfy public interest criteria set out in migration law for the grant of a visa.

1.5 When a person is listed on MAL a reason for listing them must be stated in the record. This is the primary 'Alert Reason', identifying the nature of the threat they might pose, such as *National Security*, *Serious or High Profile Crime*, *Health Concerns* or *Overstayer*. There are currently 18 different Alert Reasons, which are grouped into high, medium or low risk.[4]

What MAL is not ...

MAL is *not* a list of persons who are prohibited from obtaining a visa. Legally there can be no such list—each visa application must be considered as set out in the *Migration Act 1958*. It is incorrect, therefore, to assume that entering a person's details on MAL leads ineluctably to their being denied a visa or entry to Australia.

A person who is listed on MAL is not thereby prohibited from getting an Australian visa. Checking MAL may, however, bring potentially adverse information to the attention of the decision-maker.

A decision to grant (or to refuse to grant) a visa turns on the delegate's satisfaction that the applicant has satisfied certain criteria set out in migration law. When considering a visa application, the delegate may have information from a range of sources, including the application itself and any information brought to their attention by MAL. In making a decision, the delegate must take account of all relevant information.

MAL is a central element in border protection

1.6 DIAC has consistently described MAL as 'the department's principal electronic alert system' which, it states, 'forms an integral part of Australia's national security and border control strategy.'[5] Other major elements are:

[4] See Appendix 1. In some cases a person may also attract a further, secondary Alert Reason.

[5] See, for example, DIAC, *Annual Report 2007–08*, p. 94.

- *Australia's universal visa system.* Anyone who is not an Australian citizen and who wants to travel to Australia, enter and stay legally, must seek permission. That permission is a valid visa. Because almost all non-citizens must have a visa before travelling to Australia, DIAC can test against MAL when they apply.[6] This provides an opportunity to identify a traveller who may pose a threat to Australia before departure and minimises the possible need to turn them back at an Australian port.

- *Advance Passenger Processing (APP).* This DIAC system is used at overseas check-in to record passport details, check the visa database and DAL and issue a directive ('OK to board'/'Do not board'). This enables commercial airlines to verify that travellers have permission to enter Australia. It also sends an expected movement record to DIAC in Australia.[7] APP effectively creates an offshore border. DIAC also has airline liaison officers (ALOs) located at selected international airports.[8]

  During flight, APP checks PAL and generates an immigration directive: either to enter Australia or to refer to a DIAC officer. This directive is sent to TRIPS (see below) which forwards it to the Australian Customs and Border Protection Service's system, PACE.

- *TRIPS (Travel and Immigration Processing Systems).* This group of DIAC systems, inter alia, maintains movement records and visa information, contains copies of Australian and New Zealand passport information and has links to the APP system, MAL and PACE.

- *PACE (Passenger Analysis Clearance and Evaluation System).* At Australia's border (usually airports) Customs and Border Protection uses its PACE system to help it to clear passengers and crew across Australian borders.[9] To help Customs and Border Protection carry out

[6] A New Zealand citizen who holds a current New Zealand passport is granted a *special category visa* subject to s. 32 of the *Migration Act 1958* at the border.

[7] APP has been the subject of an ANAO performance audit: *Advance Passenger Processing* (ANAO Audit Report No.34 2005–06).

[8] DIAC ALOs are strategically located at airports with direct flights to Australia and/or last ports of embarkation to assist airlines in resolving problems with incorrectly documented passengers intending to travel to Australia. See: <http://www.immi.gov.au/managing-australias-borders/border-security/air/airlines/infringements.htm> [accessed 7 May 2009].

[9] Since 1988, Customs (now called 'Customs and Border Protection') has taken responsibility for processing everyone crossing the Australian border with delegated authority to exercise the functions of other agencies with border responsibilities.

immigration duties on its behalf, DIAC regularly provides an updated copy of MAL. PACE receives expected passenger movements and immigration directives from TRIPS. Where a directive requires, Customs and Border Protection refers passengers to a DIAC officer. PACE advises DIAC when a person has crossed the border.

- In addition, there are other layers of defence designed to identify persons of concern who are not or cannot be listed. These additional safeguards include War Crimes Screening procedures, and Police Records checks for some visa types and some tranches of applicants identified as high risk.[10]

1.7 As an essential DIAC tool, MAL must be considered in the context of the department's immigration operations generally. The volume of travellers (foreign nationals and Australians) across Australia's border has continued to rise in recent years and, in 2007–08, there were 23.6 million person-movements. Processing this increasing volume of person-movements requires DIAC to balance two contrary pressures:

> to facilitate the entry and departure of legitimate travellers whilst ensuring we detect fraud, and identify people who are not entitled to come here, locate them and stop them travelling here ... Speed and accuracy are paramount—to ensure legitimate travellers are not inconvenienced by security measures, but those who are security threats, are identified.[11]

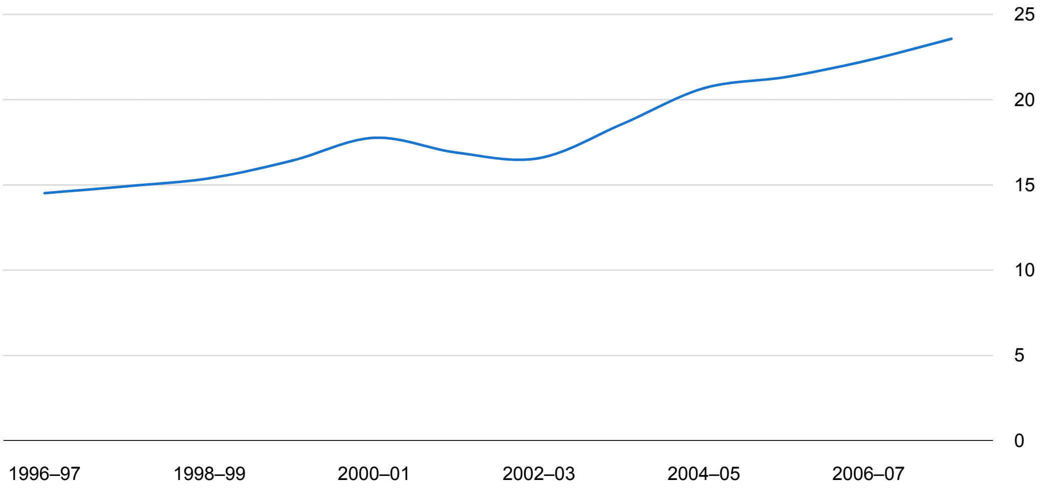
[10] DIAC advice of 19 March 2009.

[11] Secretary, DIAC, *Enhancing security through effective immigration measures* (speech to the 'Security in Government Conference', Canberra), 7 December 2007, p.2.

Figure 1.1

Number of person-movements across Australia's border, by year[12]

(Millions of person-movements/year)



Source: DIAC, Total Movements Data: <http://www.immi.gov.au/media/statistics/statistical-info/oad/totalmovs/totmov.htm> [accessed 7 May 2009]

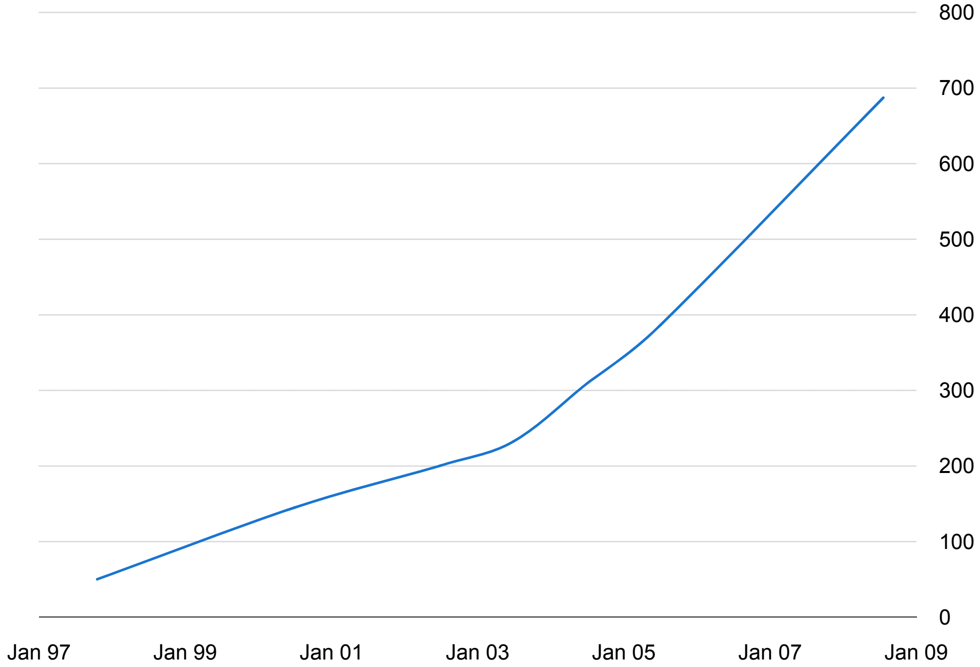
MAL's origins

1.8 MAL is based on long-established practice within DIAC. It became computerised several decades ago, when it was known as the 'Migrant Alert List'. Since then, it has developed in sophistication, significance and size. The number of records DIAC holds on MAL has risen substantially over the last ten years and continues to rise.

[12] Any changes in trend that may flow from the global financial crisis that commenced in late 2008 are not reflected in the available data, which covers the period to the end of the financial year 2007–08.

Figure 1.2

Number of persons listed on PAL, 1997–2008 ('000)



Source: ANAO analysis of DIAC data. See Table A.1, Appendix 2.

1.9 The result of both growth in numbers of movements and in numbers of persons is a commensurate rise in match notification work. DIAC reports that whereas, in 1997 there were 154 200 match notifications—possible MAL matches identified by computer for human consideration and resolution—the corresponding figure for 2008 was 3 214 000.[13]

1.10 By the mid-1990s DIAC recognised that its use of MAL had become so important that it was becoming 'MAL dependent'.[14] Moreover, MAL has accrued an increased security function after September 2001 and most of the increased numbers of records of persons on MAL are *National Security* entries. The Australian Security Intelligence Organisation (ASIO) is a key source of advice for DIAC on border security matters. It provides security assessments

[13] DIAC advice of 19 March 2009. The department advises that this 'takes account of the change in the basic metric of MAL checking in October 2007.' It forecasts that there will be 4.2 million match notifications over the financial year 2008–09 (DIAC advice of 20 April 2009).

[14] Joint Standing Committee on Migration, Australia's visa system for visitors (minutes of evidence), 1 June 1995, pp. 1152, 1155.

on selected visa applicants and unauthorised arrivals (for example, unauthorised boat arrivals).

What data does DIAC store on MAL?

(1) PAL—DIAC uses PAL to store personal identity information. PAL has the capacity to store family and given names, date-of-birth, gender, citizenship and country of birth. It can also record the visa number and travel document number of the person of interest. No other personal information (such as address) is stored. There are several fields DIAC uses for internal purposes, the most important being the narrative. This is a free-text area where the officer who creates or updates the record can write notes about the case. These provide information for a DIAC decision-maker when considering visa, entry or citizenship decisions should the PAL-listed person return a match.

(2) DAL—DIAC stores information regarding the document in question on DAL: the Document Number, the Document Type (passport or visa) and the country of document origin. No personal information—such as the name of the person to whom the document was issued—is recorded. The focus of DAL is only the document details. Like PAL, there are several administration fields including a free text narrative field.

Documents listed on DAL are usually those reported lost or stolen by the document owner, but also include lists from other countries of known fraudulent documents, primarily listed passports. Under DIAC policy guidelines, Australian travel documents have not been on DAL.[15] However, DIAC advises that it now lists Australian passports when it suspects those passports are likely to be used by an impostor. It states that this is an increasing problem as the nature of identity fraud switches from the use of false or altered documents—now increasingly subject to detection—to the use of genuine documents, improperly used. Short term listing is strictly controlled, and can only be agreed by DIAC's First Assistant Secretary, Border Security Division.

[15] The PAM3 manual states: 'Do not list Australian passports on DAL. Report any lost, stolen or fraudulently altered or obtained passports to [the Department of Foreign Affairs and Trade] for inclusion on their database as an alert.'

MAL has been reviewed, mainly internally

1.11 MAL has been the subject of five reviews over the last decade. These have been mainly internal and none has produced a public report:

- In 1998 it was the major element in *Australia's Entry Control Arrangements: a Review*, conducted by David Sadleir AO, a former Director-General of ASIO (hereafter, the 'Sadleir Review').
- DIAC itself undertook a *Technical/Operational Review of MAL* before the Sydney Olympic Games in 2000 (the 'Gerlach Review').
- DIAC's then Internal Audit and Risk Management Section completed a *Review of the Movement Alert List in a Business and System Context* (February 2003, the internal audit of MAL).
- DIAC undertook the *Review of the Purpose, Architecture and Operation of the Movement Alert List*, from September 2003 to August 2004 (the Wheen Review). This led to the CMAL development.
- In 2007, DIAC and ASIO undertook a joint evaluation of immigration-related security checking arrangements. A primary outcome of this review was the development of the Security Referral Service (SRS), which facilitates communications between DIAC and ASIO to support security checking of those who seek to travel to Australia (May 2007, the Joint Evaluation).

1.12 Although MAL has never previously been the primary subject of an ANAO performance audit, aspects have come under scrutiny in earlier audits:

- MAL was considered in the audit of *Commonwealth Agencies' Security Preparations for the Sydney 2000 Olympic Games* (ANAO Audit Report No. 5, 1998–99), *Electronic Travel Authority* (ANAO Audit Report No.3, 1999–2000) and the related *Electronic Travel Authority Follow-Up Audit* (Audit Report No.2, 2007–08);
- Because of its interactions with other DIAC systems, MAL has been mentioned in other ANAO performance audits. Recent examples are *Advance Passenger Processing* (Audit Report No.34 2005–06) and *Visa Processing: Working Holiday Makers* (Audit Report No.7 2006–07).

Management of MAL

1.13 The management challenges in the design and operation of MAL have been canvassed extensively in the various reviews mentioned above. Some aspects that regularly attracted attention have been:

- the MAL database itself, its integrity, maintenance, quality assurance of entries and its rapid growth, especially of the numbers of national security-related records;
  - National security records are different from other records in that the amount of information in each record is generally less and they usually relate to people who have not been clients of DIAC. In contrast, the non-national security records mostly relate to people known to DIAC, including previous visa applicants;
- MAL's identity-matching capability, especially the use of weaker name-matching software in offshore visa processing systems; and
- the risks of (i) having multiple copies of MAL to support DIAC's various visa-processing systems, and (ii) having MAL matches assessed by hundreds of DIAC staff in diverse locations across the world; and
- the urgency of improving reporting on performance.

1.14 Following the Wheen Review, a new policy proposal was taken to government to substantially upgrade MAL. The primary recommendation was that DIAC use a single copy of MAL, employ stronger name-matching software for all work and establish an onshore MAL centre to assess possible matches the system identifies. The resulting project, agreed by government and funded in the 2005–06 Budget, created CMAL ('Central MAL'), which was being implemented during the course of the audit.[16]

The objective and scope of this audit

1.15 The objective of this audit is to assess the effectiveness of DIAC's management of MAL. It is one of a series of performance audits examining major DIAC processes (another recent example is the performance audit of *Administration of the Health Requirement of the Migration Act 1958*, May 2007).

[16] To distinguish it from the new system the older one is referred to in DIAC as 'Heritage MAL' (HMAL).

These audits complement other performance audits of specific DIAC programs (such as *Visa Management: Working Holiday Makers*, October 2006). This audit is also part of a series of ANAO performance audits in a range of agencies focusing on client identity.

1.16 The scope of this audit is MAL as used by DIAC. It did not examine:

- private MALs. These are facilities like MAL, but separate and partitioned from MAL proper and from each other. They enable DIAC and external agencies with appropriate authority to track visa transactions and movements. In effect, private MALs offer a passive monitoring capacity. Compared with MAL, private MALs hold very few records;
- activities of agencies external to DIAC. It did not, for example, consider national security checking processes for MAL referrals by ASIO;[17]
- the SRS (see para. 1.11, above); or
- the Regional Movement Alert System (RMAS), an initiative of the Asia-Pacific Economic Cooperation (APEC) Business Mobility Group. RMAS enables participating APEC economies to conduct automated real-time checks of other participating economies' passports, verifying their status against the issuing authority's database. It currently operates among Australia, the United States of America and New Zealand.

How the ANAO undertook this audit

1.17 The audit involved examining files and records kept by DIAC in its national office in Canberra. The audit team interviewed DIAC staff and those of external agencies involved in MAL's operation.

1.18 The ANAO examined the MAL database using computer-assisted auditing techniques. Results of that analysis were provided to DIAC for consideration during the audit.

1.19 The audit was conducted at a cost of $420 000.

[17] Complaints about ASIO processing of security assessments for immigration applications are considered by the Inspector-General of Intelligence and Security.
See: <http://www.igis.gov.au/about/index.cfm> [accessed 7 May 2009].

How this report is structured

1.20 The matters examined by this audit are set out in the following nine chapters.

- The next begins with an extensive examination of the data in MAL and DIAC's management of it (Chapter 2).
- This is followed by three chapters dealing with particular matters relating to the keeping of data on MAL—controlling access to MAL (Chapter 3), the presence of records of Australian citizens on MAL (Chapter 4) and the application of privacy legislation (Chapter 5).
- Having examined the data, the report then considers the process by which it is used in visa, citizenship and border processing: the data-matching (MAL checking) process (Chapter 6).
- The report then examines how DIAC's business rules operate for MAL and whether some change would facilitate its use (Chapter 7).
- Next, the report looks at how DIAC assesses the performance of MAL both for external reporting and internal management (Chapter 8).
- Finally, it examines the project under way in DIAC since early 2005 to redevelop MAL as CMAL (Chapter 9).

How the ANAO tested the MAL data

A substantial part of the analysis in this report is based on numerous tests the ANAO performed on MAL data. DIAC provided a complete copy of the MAL database on 18 July 2008, under strict security. The ANAO loaded the database onto a secure computer on its premises. The audit team analysed the data using auditing software. Unless the context states otherwise, the tests reported here are based on a census of the records, not a sample.

The ANAO observed that the database—as of 18 July 2008—contained a total of 3 068 243 records, comprising 2 380 872 DAL and 687 371 PAL records. DIAC confirmed these numbers before any detailed ANAO analysis took place.

2. DIAC management of MAL data

This chapter considers how DIAC manages the data in MAL. This includes capturing the records that need to be placed in MAL, maintaining the database and purging it.

Why it is important that DIAC manages MAL data well

2.1 MAL is primarily a database used in conjunction with matching software. The database is at the heart of the system and its integrity, and DIAC's management of it, warrants close attention. Successive reviews of MAL have emphasised the importance of good MAL data management.[18] Taking account of those reviews, the ANAO considered the following matters to assess how well DIAC manages MAL data. Each is examined in detail below.

(1) *Populating MAL*—First, DIAC should have a sound strategy for populating MAL. For MAL to be effective, DIAC must be assured it contains the right records: that is, records of relevant persons and documents. This is a continuing task as MAL records are constantly being added, deleted and changed—thus there is never a static set of the 'right' records.

(2) *Ensuring that MAL records are complete and accurate*—Second, DIAC should be confident that MAL records are as complete and accurate as possible. The better the quality of the data held the better the chance of making a sound match. Moreover, records with sparse or wrong data can yield multiple possible matches of poor quality, which require time to consider, with infrequent reward and adding to the cost of administration.

(3) *Reviewing and deleting MAL records*—Out-of-date and unnecessary records slow the matching process and add unnecessarily to processing costs. Therefore, to optimise processing efficiency, DIAC should seek to purge MAL of such records.

[18] The Sadleir Review (p. 16) stated that 'Because MAL cannot be better than the information it contains it is of the first importance that the data it contains be as accurate as possible.' The Wheen Review (p. 57) found that the quality of the data—in both coverage and content—cannot be over-emphasised.

(1) Populating MAL

The need for a plan to populate MAL

2.2 For MAL to work effectively, it must contain all the right records: that is, records of all relevant persons and documents. Only when a record of a person who poses a threat to Australia or suspect travel document is recorded in the database can DIAC expect MAL to yield a match. The more complete MAL is and the more promptly updated, the lower the risk of a person who poses a threat to Australia escaping detection. On the other hand, as earlier reviews have emphasised, the fewer records, the greater the efficiency of processing.[19] Balancing costs and risks means that the comprehensiveness of the database needs to be carefully considered.

2.3 The Wheen Review, which found that many sources for MAL entries were ad hoc, recommended that DIAC develop a plan—within an overall MAL strategic plan—to identify sources and, where possible, systematic processes for entering such information into MAL.[20] DIAC could set out how it would strike a balance between risks and costs in such a plan. The recommendation was agreed and funded by government.

2.4 As MAL's purpose is to draw information to a decision-maker's attention relevant to their decision, that information must be soundly-based.[21] Only then can it be relied on. Therefore, records must be selected for inclusion only where there is credible evidence for the contentions made.

2.5 To examine whether DIAC manages the populating of MAL effectively the ANAO considered the following:

(a) whether DIAC has developed a central plan to populate MAL;

(b) whether DIAC has controls on the promptness of entering data;

[19] Sadleir stressed the need to keep the number of MAL records to an essential minimum. (Sadleir Review, p. 18.) Also, in Parliament, the then Attorney-General rejected the idea that Australia should seek to include in MAL wholly comprehensive lists of every possible person of potential concern. See Hansard, House of Representatives, Questions without Notice, 3 November 2003.

[20] Wheen Review, pp. 79–81. CMAL project management planning documents acknowledge that this recommendation was funded. DIAC, 'Central MAL Project—Project Management Plan', (Final V3.0), 21 July 2006; 'Traceability Matrix for Defining CMAL Project Scope', May 2006.

[21] See Administrative Review Council and DIAC, *Decision Making: Evidence, Facts and Findings* (Best-practice guide 3), August; and DIAC 2008, *Good Decision Making: Training for DIAC Decision Makers*, Version 1.08, April 2007.

(c) the continued existence of old records based on allegation or suspicion;

(d) whether MAL records generally refer to evidence and credible sources;

(e) the existence of easily-detectable records of questionable merit; and

(f) DIAC's handling of records it obtains from open sources.

(a) DIAC has not developed a central plan to populate MAL

2.6 DIAC has prepared no overall MAL strategic plan, envisaged by the Wheen Review, nor any subsidiary plan for populating MAL.[22] The department ascribes responsibility for managing PAL data to Alert Reason owners,[23] mostly comprising various parts of DIAC but also other Commonwealth agencies. It has no written statement of Alert Reason owners' responsibilities, but some have mechanisms to populate MAL with records of primary interest to them.[24] This is much the same state of affairs as the Wheen Review found in 2004:

> Only a few of MAL's current information sources provide data which goes into the system in a systemic [sic] way. It is notable that it has been the PAL [Alert Reason] codes which have been populated in a systemic fashion which have grown most significantly in recent years.[25]

2.7 Generally, DIAC Alert Reason owners see their role as to develop policy as to who should be listed.[26] That is reflected in DIAC's detailed PAM3 manual. The onus is then on DIAC staff to enter records when appropriate.

2.8 *National Security* records have formed the majority of new entries for PAL records since about 2001. DIAC advised that its efforts in this context have been focused on quickly entering and providing reporting on substantial additional tranches of *National Security* records ever since.[27]

[22] DIAC provided the *MAL Review Implementation—Project Sponsor Report* (current as of July 2008) which updates progress with each recommendation flowing from the Wheen Review. In relation to the relevant recommendation, it provides only references to some individual activities in relation to populating the DAL part of the database.

[23] DIAC email advice of 2 May 2008.

[24] For example, some have arrangements with external agencies. DIAC's War Crimes Unit receives listings from the Department of Foreign Affairs and Trade of suspected war criminals published by international tribunals and similar bodies, and enters them into PAL (DIAC email advice 18 July 2008).

[25] Wheen Review 2004, p.79.

[26] DIAC email advice of 22 and 27 May 2008.

[27] DIAC advice of 19 March 2009.

Opportunities to populate PAL have been identified previously

2.9 A recent ANAO performance audit report[28] suggested that people who have made health undertakings be MAL-listed. Typically 13 500 to 22 000 health undertakings are issued each year.[29] Placing known cases on MAL could inform future visa decisions, and allow DIAC to remind applicants of pending health undertaking requirements. It is an example of how the *Health Concerns* Alert Reason owner could actively populate MAL based on credible information. Currently, where a visa holder is non-compliant with their health undertakings, DIAC makes no MAL entry for its future reference.

2.10 DIAC was considering entering records into MAL based on active health undertakings in May 2008.[30] It advised that it had updated the Health part of DIAC's PAM3 manual, putting the onus on the client contact officer to place a record on MAL. DIAC would automate the process by July 2009.[31]

There is no systematic approach to populating DAL

2.11 The Wheen Review characterised DIAC's inclusion of data in DAL as 'opportunistic'. Various government agencies provided the data at their discretion mainly with no formal agreements.[32] Data collection for DAL had developed piecemeal with no strategy and no structured or formal approach to other governments or agencies to obtain data. There were no MOUs (memoranda of understanding).[33] Acquisition was 'to a significant extent based on relationships which individual [DIAC] officers have developed with host governments.'[34]

2.12 The Wheen Review stated that the existing DAL records represented 'only a small percentage of the travel documents that [DIAC] would be inter-

[28] ANAO Report No.37 2006–07, *Administration of the Health Requirement of the Migration Act 1958,* tabled 17 May 2007.

[29] ANAO Report No.37 2006–07, p.111. Current analysis of MAL found 2379 records with the term 'Health Undertakings' in the narrative, of which DIAC had entered 620 after May 2007. This suggests that only a small proportion of current health undertakings are entered into MAL.

[30] DIAC, Internal minute from Assistant Director, State and Territory Health Liaison, 20 May 2008.

[31] Automation will be under DIAC's major systems redevelopment, *Systems for People* (SfP) program Release 9 (DIAC advice of 22 January 2009).

[32] Wheen Review, Appendix 2, 'Deliverable C8', p. 133.

[33] Ibid, p. 142.

[34] Wheen Review, para. 9.9, p. 52

ested in.'[35] The same review concluded it worthwhile for DIAC to target countries for formal data exchange agreements. It recommended that DIAC 'develop a plan to identify sources of entries and where possible establish systemic [sic] processes for entering such information on MAL.'[36]

2.13 During the audit, DIAC stated that the current position is:

> We rely on overseas posts, law enforcement agencies and STOs [*State and Territory offices*] to report all lost, stolen and or fraudulent travel documents to the department for listing. *We accept whatever we are given* by foreign governments and local sources which is loaded on the system with a short turnaround time [emphasis added].[37]

2.14 The active, systematic strategy for populating DAL envisaged by the Wheen Review has not been implemented. Populating DAL remains passive—'accepting whatever we are given'—and indistinguishable from the position before that review.

(b) DIAC has no controls on the promptness of entering MAL data

2.15 As well as collecting all the right records to populate MAL, DIAC must also ensure it enters them promptly into the system so they are available for checking. Otherwise there is a risk, for example, that a person who could have been MAL-matched will seek to travel to Australia before MAL has been updated and MAL will not be able to fulfil its alert function.

2.16 There is no specific instruction in DIAC's PAM3 manual as to how promptly MAL records must be entered although it does state that existing records 'must be updated as new information comes to light.'[38] DIAC advised: 'The time between the need to create a record and its creation in MAL is an issue for discussion with the relevant business area.'[39] However, as there is no written statement of Alert Reason owner responsibilities, accountability for this aspect is unclear.

[35] Ibid, p. 133.

[36] Wheen Review, para. 15.14, p. 81. This was part of the new policy proposal agreed by government in the 2005 Budget.

[37] DIAC, email advice, 20 June 2008.

[38] DIAC, PAM3, GenguideA—MAL (Movement Alert List)—Policy and procedures, p. 73.

[39] DIAC, email advice, 27 May 2008.

(c) Old records based on allegation or suspicion remain in MAL

2.17 DIAC's PAM3 manual provides instructions for staff on the creation of MAL records: 'The creation of a MAL record must be on the basis of evidence from a credible informer.'[40] This implies two necessary tests for the creation of a MAL record: evidence and a credible informer.

2.18 DIAC instructions in earlier years were less demanding. The *Migration Series Instruction 197* (MSI 197) of April 1998 states:

> MAL includes alerts on the basis of allegations or suspicions, as well as proven factual information, from a variety of sources and of varying credibility. Because its primary function is to alert decision-makers to information, not determine their decision, the evidence and procedures required to lawfully make a Migration Act or Citizenship Act decision do not apply to the creation of a MAL alert.[41]

2.19 Current instructions do not reflect these views. DIAC advised that the change in policy on evidentiary requirements occurred when it reviewed the MAL instruction in the follow-up to the Wheen Review, and 'after a number of client service issues related to non-substantiated MAL entries had occurred.'[42]

2.20 The audit found no evidence that records that may have been entered on the basis of allegation or suspicion before that policy change have been removed systematically. This means that DIAC has no assurance that some do not remain.[43] The audit was able to identify potential instances of such records.

(d) MAL records generally refer to evidence and credible sources

2.21 The ANAO examined MAL records to see if it could determine, prima facie, whether the record showed that it came from a credible source and was based on evidence.[44] First, it examined DIAC's use of the 'informer code' field in each MAL record, which is intended to show the source of the information.

[40] The informer is the person or organisation that is the source of the information placed in the MAL record.

[41] MSI 197, 9 April 1998. MSIs have been updated and incorporated in the PAM3 manual in recent years.

[42] DIAC advice of 22 January 2009.

[43] The ANAO counted some 52 994 active PAL records that were created before 31 December 1998.

[44] DIAC's primary sources are its staff, its own records, advice from other Australian departments and agencies and foreign governments. For practical purposes, this analysis has taken references to DIAC's own other records in its visa and citizenship processing systems and information from any official source external to DIAC as trustworthy. That is, for example, where a record indicates that advice derived from Interpol advice audit testing did not verify that with Interpol.

Then it examined a random sample of PAL and DAL records to test for the existence of a source and an evidentiary basis by inspection of the record.

(i) DIAC has been increasing its use of the informer field

2.22 The Wheen Review found the informer field to be 'distinguished by its lack of use'[45] and concluded:

> [DIAC] is not currently able to accurately identify the entries from a particular agency or source. This situation could be remedied by the use of the current 'Informer Code' field on MAL. The purpose of this field is to report on the number of entries sourced from a particular agency ... [It] should be made ... mandatory.[46]

2.23 DIAC has not ensured that the informer field has been consistently completed when records have been entered into MAL. Although the Wheen Review proposed this be addressed in 2004, the frequency with which this field is completed is at about 14 per cent for PAL and 42 per cent for DAL. However, the analysis shows that, for both PAL and DAL, the trend is for a higher proportion of new records to include this information.

2.24 DIAC stated that it 'is not possible' to implement the Wheen recommendation 'as CMAL is tethered to HMAL [Heritage MAL]',[47] implying that it will be possible only now that DIAC has implemented CMAL. However, even if it has been impracticable over the last four years to make the software *mandate* that this data be entered, there is no obvious reason why DIAC could not have *instructed* its staff to do so. It remains optional in DIAC's instructions.

(ii) Inspection shows records generally refer to evidence and credible sources

2.25 Given that the informer code field has not always been completed, the ANAO examined a random sample of MAL records to see if, regardless of the infrequent use of this field, the source of the information could, in any case, be identified. This largely involves determining whether the source is clear from whatever has been written in the 'free-text' portion of each MAL record, the narrative. The ANAO did this by inspection, at the same time as examining the record to see if it contained an indication of an evidentiary basis.

[45] DIAC, MAL Review Internal Working Documents, p. 11.

[46] Wheen Review, p. 81.

[47] DIAC, MAL Review Implementation—Project Sponsor Report, July 2008.

2.26 Testing showed with a high degree of confidence that the number of MAL records where it is not possible to discern an informer and identify an evidentiary basis is only a small minority. The proportion of DAL records where it is not possible to discern an informer and identify an evidentiary basis is smaller still.[48] Nevertheless, during its analysis the ANAO came across a small number of records whose evidentiary basis was questionable.

(e) Inspection can easily detect records of questionable merit

2.27 Analysis identified a small proportion of PAL records with a blank narrative. *National Security* records generally do not contain information in the narrative.[49] However, there were also 142 non-*National Security* PAL records with a blank narrative.[50] If there is nothing in the narrative in these cases then there is no information to show the basis on which the record has been placed on PAL. Such records can serve no useful function.

2.28 Second, DIAC's PAM3 manual now requires that persons must not be listed on the basis of allegations unless the allegation is from a credible informer and can be reasonably justified. It warns against inclusion of impressions, interpretations or information implying contingency or uncertainty about the circumstances of the person being referred to.

2.29 The ANAO reviewed PAL records to see if it could identify instances of inappropriate narratives. This included searching for the use of terms implying uncertainty.[51] Individual inspection is necessary to see the context in which the terms are used, as their mere use does not mean the record is unsound.

2.30 Inspection identified instances of adverse information in a narrative based on allegations and not supported by substantiating material or a reference to a verifiable source. For example, a record dating from 2001 states:

[48] It can be said with 95 per cent confidence that the proportion of PAL records for which it is not possible to discern an informer and identify an evidentiary basis is not greater than 8.92 per cent. Similarly, it can be said with 95 per cent confidence that the proportion of DAL records for which it is not possible to discern an informer and identify an evidentiary basis for the record is not greater than 4.66 per cent. These results are based on inspection of a random sample of 100 cases in each of PAL and DAL.

[49] As any relevant information will be retained by security agencies and can be referred to as necessary when a match occurs, this absence is unimportant.

[50] These 142 records have been created since 1 January 2005. The ANAO referred these records to DIAC for its consideration and DIAC advised that, by January 2009, it had reduced this number to 51. A similar number of DAL records with blank narratives exist.

[51] This technique—searching the narratives for key words to identify records that need attention—has also been employed by DIAC, for example, in its ongoing clean-up of *Health Concern* PAL records.

> INFORMATION REC'D [*DATE*] FROM A COMMUNITY SOURCE ALLEGING THAT [*ABOVE NAMED]* HAS AN EXTENSIVE CRIMINAL RECORD IN [*ANOTHER COUNTRY*] – B[*OR*]N IN TOWN OF [*TOWN NAME*] IN VICINITY OF [*CITY NAME*], SON OF [*NAMES*]. HE HAS BEEN ILLEGALLY IN THE USA FOR OVER 12 YRS AND WILL TAKE ADVANTAGE OF RECENT AMNESTY ANNOUNCED IN USA TO ACQUIRE GREEN CARD. SOURCE FEARS HE WILL THEN SEEK TO ACQUIRE [*AUSTRALIAN*] VISA AND WILL NOT DISCLOSE [*NATIONALITY*] CRIMINAL RECORD. [*ABOVE NAMED*] HAS ALLEGEDLY MADE NUMEROUS DEATH THREATS TO MEMBERS OF THE AUSTRALIAN COM[*MUNITY*(?)][52]

(f) Records DIAC obtains from open sources require more care

DIAC proposed using open-source information nearly a decade ago

2.31 Over a decade ago, Parliamentary consideration of the origin of a MAL record raised doubts as to the appropriateness of open or public sources for MAL entries.[53] Subsequently DIAC spent three months investigating the possible use of open source information (OSI). It sought the agreement of the then minister to establish a central OSI unit to obtain information from Internet sites of established integrity to populate MAL. DIAC expected the project to result in the details of about 500 known criminals being added to MAL.[54]

2.32 It is not clear what happened as a result of this project: DIAC is unable to locate any further information on it.[55] However, the department had originally intended to use a specialised unit to gather data from such sources. DIAC has now given authority to enter data into MAL sourced from the Internet to its 4000 or so users throughout the department.

DIAC's current approach

2.33 The PAM3 manual encourages DIAC officers to derive information to populate MAL from diverse sources, including reputable web sites, media reports and non-government agencies.[56] It also requires officers wanting to

[52] Items in brackets indicate where an abbreviation in the original has either been interpreted or specific detail replaced with more general information.

[53] See Senate Estimates hearing of 21 August 1997, pp. 70–1, at which Senator McKiernan raised this issue with DIAC officers, who agreed that they should have used authoritative rather than public sources for certain information that DIAC had entered into MAL.

[54] DIAC, minute to the Minister, 19 November 1999.

[55] DIAC advice of 22 January 2009.

[56] DIAC, PAM3, GenGuideA—Movement Alert List—Policy & Procedures, section 19.5, 1 December 2007.

enter such records to discuss it with a supervisor or with CMAL Operations Section and state the information and sources in the narrative.[57]

2.34 DIAC analysed MAL records in November 2006 as part of a program to identify poor data quality and found:[58]

> Another concern is reliability of sourced information with some records found to have references to local newspapers, not only Australian newspapers, and websites which are not known reliable sources e.g. sites created by non government independent groups which do not always contain factual information but instead advocates opinion or unsubstantiated facts. *During the BOC [Border Operations Centre] training attended by the Data Analysis Team and other new starters in the BOC, it was conveyed to all staff that they could "Google" to gain more information for alerts.* The creation of such records also leaves the Department vulnerable to legal action if the information is requested under the Freedom of Information Act. This also brings into question the integrity of the MAL/CMAL system [Emphasis added].

2.35 DIAC's analysis did not specify how often it identified such records. It recommended a new procedure in which Alert Reason owners would validate sources. This was followed up in January 2007, when DIAC's CMAL Practice Management Group considered a minute on unsubstantiated PAL records:

> This issue raises concerns for the legality of some of the records currently on MAL. For example, records have been found to have very little substance in the reason for listing a person. In some cases [DIAC] staff have taken information from websites not generally considered as reputable by [DIAC] and used this source to create or update a MAL record.[59]

2.36 The same minute reflected the view that Alert Reason owners are responsible for data quality. It proposed the Group 'monitor progress of data cleansing.' However, DIAC later disbanded this group. It has advised recently that it will set up a new body to progress data ownership and quality.[60]

2.37 The CMAL Data Management team has done more reviews of data quality recently. In July 2008 it found that the 'Character [*Section of DIAC*] has

[57] Ibid., section 19.2.

[58] The analysis examined the use of the Remote Input Function (RIF) for entering MAL data. See DIAC, CMAL Data Analysis Team, Internal Database Analysis, 'Remote Input Function (RIF) – Analysis', undated but estimated to be circa December 2006 – January 2007.

[59] DIAC, minute of 17 January 2007, to the CMAL Practice Management Group.

[60] DIAC advice of 22 January 2009.

been aware that there are a [*unspecified*] number of records that refer to vigilante websites as the source of data in the narrative.'[61] This is another reference to records being entered from the Internet with insufficient evidence.

2.38 DIAC stated that getting data from the Internet remains problematic:

> Decisions concerning the use of information from external sources including the internet will remain a matter for judgement and the employment of some basic safeguards to test the veracity of the information and seek additional information such as more accurate biodata or narrative on why an identity should be listed. We would propose to address this directly though enhancements to the MAL PAM advice and in training for DIAC staff in the entry of information into MAL.[62]

2.39 DIAC also stated that it 'is not currently resourced to deal with the management of a wide range of external sources'.[63] Doing that was one of the recommendations of the Wheen Review, proposed to and funded by government in 2005.

Conclusion—populating MAL

2.40 There are opportunities for DIAC to:

- consider, once again, whether it would benefit from preparing a central plan for populating MAL; and
- impose a quality assurance regime on the existing stock of MAL records using selected terms as a means of identifying PAL and DAL records that need further follow-up to ensure either that evidence is included or the record deleted. Such an approach will not exhaustively identify all records in need of attention but should help to deal with the majority of such records.

2.41 Both of these ideas would best be considered in the context of a risk analysis for the future operation of MAL and are predicated on resolving satisfactorily questions of ownership and responsibility for the data.

[61] DIAC, CMAL Data Management Team, 'Data Quality Overview: Character', circa 23 July 2008.

[62] DIAC advice of 22 January 2009.

[63] DIAC advice of 22 January 2009.

(2) Completeness and quality of MAL records

The risks of MAL records being incomplete

2.42 DIAC recognises that, for MAL to work as effectively as possible, the records should be as complete as they reasonably can be.[64] An incomplete individual record is one which, for example, might contain a surname but lack a given name; or the person's citizenship may be unknown or dates are absent or only partially known. DIAC's instructions to its staff state:

> Although all [Alert Reasons] have a minimum data standard, staff are encouraged to populate as many fields as possible as this will significantly improve data quality and subsequent MAL checking processes.[65]

2.43 MAL records 'owned' by DIAC should have a narrative that is accurate, up-to-date, relevant and complete.[66] This enables a decision-maker to proceed efficiently to finalise the matter before them. Deficient or obscure narratives will add delay as they resolve whether there is substance to an alert.

2.44 Other risks of incomplete and poor quality records are:

- multiple possible matches of poor quality when the MAL system tests a person's data against its records; In particular, poor quality records increase the numbers of possible matches with relatively few actual matches resulting. The most recent review encompassing MAL, the Joint Evaluation, noted that the ratio of potential to actual matches:

  > suggests a very high level of wasted work. Moreover, it creates a 'fog' through which it can be difficult for an operator to see whether there is an actual match amongst the large number of potential match notifications

- uncertainty in the mind of the officer considering a possible match as to whether it is, in fact, a true match (and consequential increased risk of admitting a person who poses a threat to Australia or delaying a genuine traveller);

[64] It should be noted that the previous section of this chapter considered the completeness of MAL as a *database*: that is, it considered whether all the records that should be in MAL are there. This section also deals with completeness of the information in MAL but in a different sense. Here we are concerned with whether the individual *records* that are in MAL have all the data in them that they should.

[65] DIAC, PAM3, GenGuideA – MAL (Movement Alert List) – Policy & Procedures, 1 December 2007, p. 54.

[66] As mentioned earlier, MAL *National Security* records do not contain information in the narrative.

- greater time and resources required of DIAC officers to resolve the larger number of possible matches thrown up by the system;
- vigilance fatigue among those officers from the infrequency of true matches in very many possible matches (and consequential increased risks of missing a genuine true match); and
- loss of credibility of the MAL system as a whole.

2.45 Although there is a strong imperative for DIAC to keep MAL records as complete as is practicable, there are also risks in failure to keep records where the information is sparse. It may be better to have a sparse record of a person of concern than none at all if that helps prevent an adverse incident. Thus, decisions on what records to include require careful risk management.

Previous analysis of the quality of MAL data

2.46 Every review of MAL has considered the quality of MAL data. In particular, the internal audit of MAL focused on the quality of narratives and suggested that they be monitored by the DIAC National Office section responsible for MAL. In addition, it concluded:

> Aside from some data cleansing activities, the core data is not reviewed by 'owners' of the data. If data owners reviewed entries there may be benefit in ensuring that redundant data is not kept and that the MAL entry is of a particular standard. Certain [*Alert Reasons*] are identified with particular [*DIAC*] areas or external agencies, an annual review of MAL entries by these areas may assist in ensuring that MAL only contains up-to-date and relevant information.[67]

2.47 The internal audit of MAL recommended DIAC 'consider the feasibility of an annual data review by relevant data owners to ensure MAL entries are up-to-date and meet data quality standards.' DIAC management agreed, stating that:

> Review periods are set in consultation with data owners when records are added to MAL and the adequacy of the alerts is closely monitored to ensure best possible data ... Functionality already exists in MAL to identify records that are deficient in data and referral processes exist for the evaluation and

[67] DIAC, Internal Audit: Review of the Movement Alert List in a Business and System Context, p. 19.

> update of these records for continuing relevance. [DIAC] will consider the costs and benefits of conducting additional reviews of MAL holdings.[68]

2.48 In fact, there is no known capacity in MAL to identify data-deficient records.[69] Furthermore, there have been no annual data reviews by data owners to meet quality standards even though the CMAL Data Management team has analysed the database extensively in the last two years.

2.49 The subsequent Wheen Review (2004) recommended that DIAC 'aggressively promote with [*its*] officers the negative consequences for the operation of MAL of inaccurate and incomplete data being included in MAL.'

Current analysis of the quality of MAL data

2.50 To assess whether DIAC ensures MAL records are complete and accurate, the ANAO considered the following:

(a) whether DIAC has determined which data it needs;

(b) the limitations of the mechanisms DIAC has used to enter data;

(c) whether DIAC has sought to analyse its own data;

(d) whether DIAC has systematically addressed data quality deficiencies;

(e) how MAL data quality has changed in recent years;

(f) DIAC's quality assurance function for the data; and

(g) some instances of inaccurate and deficient records in MAL.

(a) DIAC has determined which data it needs

2.51 DIAC has had minimum data standards (MDS), for each Alert Reason in PAL since at least 1997.[70] DIAC has set out these MDS in a table, showing, by Alert Reason, which are required among a set of fields: year of birth, date-of-birth, sex, country of birth and country of citizenship. For some Alert Reasons, any of several combinations of these fields satisfies the MDS. However, in each case, the MDS merely specifies, by Alert Reason, which

[68] DIAC, Internal Audit: Review of the Movement Alert List in a Business and System Context, p. 20, Recommendation 9.

[69] DIAC has not been able to advise of any such functionality (DIAC advice of 22 January 2009).

[70] DIAC, email advice of 5 June 2008.

fields are required to hold data. Thus they relate to the presence of data and not the quality of that data (such as dates being within particular ranges).

High risk cases require less detail

2.52 High risk records require less data than low risk ones. This is a matter of judgement with risks on either side. Rejecting sparse records risks missing a match—accepting them generates more work for a few extra 'hits', slows performance and lowers service levels.[71] In practice:

(1) low and medium-risk records originate with DIAC and should be complete, as DIAC is likely to have complete data on the person;

(2) high risk records, many of which come from security agencies, may be sparse but judged sufficiently valuable to warrant entering into MAL.

2.53 DIAC has recognised the significance of the trade-off. It identified as a potential challenge for MAL's future operation 'a return to reliance on poorer quality records (conservatism in ensuring that any possible identity is listed regardless of the value of the record)'. It foresees a risk of this in the event of a major incident or perceived threat.[72]

2.54 DIAC states that it has worked with security agencies establishing appropriate MDS (following the Joint Evaluation in 2007) and applying them to both the existing stock of *National Security* records in MAL, and to new records to be loaded into the database.[73]

2.55 DIAC takes a cautious approach to MDS, advising that it:

> does not agree that minimum data standards should be made mandatory or rigidly adhered to as this would work to discourage officers from entering information which, even though it may appear deficient, may be sufficient to alert a decision-maker to undertake additional checking or exercise additional caution when approaching a decision which may affect a client.

2.56 The department states that the 'enforcement of mandatory as opposed to voluntary data standards ... could conceivably discourage staff from entering information which will prove to be of value.'

[71] The absolute minimum amount of data required to create a PAL record is *Family Name* and *Year of Birth*, with a dash in the *Given Name* field (DIAC, email advice of 15 July 2008).

[72] DIAC advice to the ANAO at the commencement of the audit.

[73] DIAC advice of 19 March 2009.

2.57 DIAC has provided an example of a set of identities of non-citizens supplied by another Commonwealth agency where the persons concerned would be affected by travel sanctions the Australian Government had decided to impose. The original list, though sparse in data content, was compiled and loaded promptly to ensure government's expectations could be met. DIAC also provided a 'current and mature' list covering the same group, which provides more comprehensive information for each person-record.[74] The department attributes the better information to ongoing engagement between DIAC staff and those of the other agency.

2.58 These circumstances show that there is a case for entering identities into MAL with only sparse data. Such an approach is consistent with the goal of maximising the likelihood of identifying a non-citizen of concern travelling or seeking to travel to Australia. Nevertheless, under this approach, it is important to have in place appropriate arrangements to review such records over time so that there is follow-up, as took place in the circumstances described above. This might mean, for example, that a flexible approach to meeting MDS is permitted at original entry of a new record and tolerated for a set period, after which the merit of the record is reconsidered.

(b) The mechanisms DIAC has used to enter data have limitations

2.59 DIAC has used four separate methods to enter data into MAL:

- bulk loads of extensive sets of data obtained from external sources, which it describes as an 'archaic and time intensive process';[75]
- entries made by its Entry Operations Centre (EOC)[76] using information provided by staff and other users;
- the CRUD (Create, Review, Update and Delete) function, which allows the user unrestricted control of the process; and
- the Remote Input Function (RIF), introduced in September 2001. This allows staff to enter records which are routed first to the EOC, whose staff are expected to check data quality before entry into MAL.

[74] DIAC advice of 20 March 2009, 'Examples of Improvements to MAL Datasets Over Time'.

[75] DIAC, email advice of 28 October 2008.

[76] DIAC's Entry Operations Centre (EOC) is a 24 hours-a-day help desk which provides advice to resolve problems that arise at ports and the border. The EOC has also entered a proportion of MAL records from information provided by other staff.

2.60 Successive reviews have recommended greater use of the RIF. The 2003 internal audit of MAL recommended that DIAC consider making it compulsory as it provided a superior audit trail, and less double handling. The Wheen Review proposed that DIAC 'aggressively pursue expansion of use of the RIF.' Although it made no formal recommendation, its final report saw the RIF as a valuable innovation enhancing data quality, and stated:

> action should be taken to ensure that use of RIF is much higher than the current levels of only half of entries which could be made by this process.

2.61 It is not clear how successful DIAC has been in maximising the use of the RIF. However, the CMAL Data Analysis Team has cast doubt on the quality of data entered by this method. It attributed poor quality data both to poor original entry by RIF users and to quality checks in the EOC being inadequate. A minute to the CMAL Practice Management Group stated: 'The quality of records originating from RIF users is poor and in some cases not useful for the purpose of making concise decisions and is not in accordance with [*the*] PAM3 [*manual*].'[77]

2.62 Thus, although the RIF introduced some discipline on data entry, this was insufficient to ensure adequate data quality. After further analysis of data quality, the CMAL Data Management Team suggested quality assurance for PAL data entered through the RIF could be improved, and questioned whether the EOC undertakes any quality assurance at all.[78] DIAC advised later that the RIF 'allowed for limited checking of the supplied data and lacked the controls to ensure that full and proper review of proposed records would take place.'[79]

2.63 DIAC advised in April 2009 that it had introduced:

> new and more rigorous oversight of the entry of new information into the CMAL database with the implementation, in March 2009, of a new Remote Input Function (RIF) for CMAL replacing the older MAL version of RIF. The new RIF provides a more effective way for new records to be proposed, while the edit/review function for new records entered through the RIF has now been transferred from the Entry Operations Section to the CMAL Operations Section, to allow for a higher degree of focus on quality issues.[80]

[77] DIAC, minute, 17 January 2007, to the CMAL Practice Management Group.

[78] DIAC, CMAL Data Management Team, 'Data Quality Overview ARC 05 09 25—Character', note circa July 2008.

[79] DIAC advice of 16 February 2009.

[80] DIAC advice of 20 April 2009.

(c) DIAC has sought to examine its own data

The data mining project

2.64 In September 2005, DIAC developed a proposal for its 'data mining and statistical risk analysis project'. It sought to achieve a 'greater understanding of the characteristics of the [MAL] database ... to help make informed decisions about improving MAL searches and reducing the number of false positive matches without loss of true matches.'[81]

2.65 DIAC engaged consultants to review the MAL data in April 2006, and again in June 2006. These reviews provided a *value analysis* of the data—counting the numbers of records per field/category, numbers of blank records or void/null records. They did not test MAL against the business rules set out in DIAC's PAM3 manual.

2.66 Comments by experienced staff in the MAL area record that they did not perceive that DIAC derived much value from the analysis.[82]

DIAC put in place a MAL data management/quality team

2.67 When preparing to migrate data from HMAL to CMAL, DIAC put in place a data management team to do structured analysis of MAL data quality. The CMAL Data Quality Project analysed PAL records to identify data quality deficiencies among bio data and narratives. The aim was to amend or remove data inconsistent with business rules or of no aid to decision-makers:[83]

> Our key objective is to review all MAL alerts by the time we transition [sic] to Central MAL in April 2007. We are focusing on ensuring that all data quality initiatives are undertaken between October 2006 and December 2006.[84]

2.68 The project produced a range of 'Internal Database Analyses', mostly by Alert Reason. Typical analyses examined whether the data met minimum data standards, whether review codes were sound, whether data was present in various fields and, in some cases, made recommendations for improvement. However, Border Security Systems Branch took the view that:

[81] DIAC, internal minute from the CMAL Section, 22 September 2005.

[82] DIAC, Data Demographics Report—Comments, circa May 2006.

[83] DIAC, minute of 17 January 2007 to the CMAL Practice Management Group.

[84] DIAC, email from CMAL Operations to Character Assessments and War Crimes Screening Branch, 28 September 2006.

> The CMAL Data Analysis Team cannot make the changes to PAL records where the Alert Reason Code (ARC) is owned by other business areas, their responsibility extends to recommending improvements and changes based on analysis of records within MAL.[85]

2.69 Most of DIAC's data quality management efforts during the period since September 2001 have been focused upon *National Security* records, which comprised over 55 per cent of PAL records in July 2008.[86]

(d) Attempts to address data quality deficiencies have had variable success

2.70 The Joint Evaluation (May 2007) made a range of recommendations to improve MAL processes, including reassessment of the value of some records listed, review of data standards and a cull of data deficient or irrelevant records. DIAC states that it has since worked to ensure that minimum data standards are maintained for *National Security* records and regular 'bulk delete' processes are undertaken to remove records considered too sparse to be of value. DIAC also reports that, in the light of the recommendations of the Joint Evaluation, on 21 August 2007, some 45 000 records were deleted from the PAL.[87] However, as noted below, the proportion of data deficient *National Security* records has increased substantially between 2003 and 2008.[88]

2.71 In 2008, the CMAL Data Management team began systematic engagement with DIAC Alert Reason owners to improve the quality of existing MAL records originating within and 'owned' by the department.[89] Evidence of actual progress exists only for *Health Concerns*.

2.72 Action to improve the quality of existing *Health Concerns* PAL records began in January 2008.[90] Health Policy Section was concerned that clients who were the subject of a health undertaking were placed on MAL on an ad hoc

[85] DIAC, minute of 17 January 2007 to the CMAL Practice Management Group.

[86] See Appendix 2, Table A1. DIAC reports that this proportion had reached 59 per cent by the end of February 2009 (advice of 19 March 2009).

[87] DIAC advice of 19 March 2009. These deletions took place before the audit commenced. DIAC also provided advice of periodic activities since 2004 directed at data quality of *National Security* records. Many of these centred on 'bulk load' and 'bulk delete' processes.

[88] See Appendix 2, Tables A4 and A5.

[89] DIAC, CMAL Data Management Tasklist, May 2008.

[90] DIAC, internal minute, *CMAL Data Management Team—Data Quality Overview ARC06 – Health* (plus a series of other similar analyses).

basis and rarely deleted.[91] That section (the 'data owners') and the CMAL Data Quality team undertook a review to delete out-of-date records.[92]

2.73 About 3000 records were reviewed in May – June 2008, leading to the deletion of over half.[93] However, Health Policy Section said in June 2008 that it did not have any continuing capacity to review large volumes of records, although it could review a few. At the same time, it 'expressed concern that RIF entries are not adequately quality assured, because records containing 'please delete' in the narrative continue to get loaded into MAL.'[94]

2.74 During the ANAO's review, the Character Transition Taskforce Section of DIAC's Compliance and Integrity Support Branch stated that, for the character Alert Reasons, the guidelines for creating and updating records are set out in the PAM3 manual. However: 'the character related procedures are soon to be reviewed by our section to improve data quality and overall effectiveness of records on MAL'. It went on to say:

> The Character section is classed as the 'data owners' of the above category of [Alert Reasons], however [it] does not review or QA entries. We see this as a major issue and as such will look at ways of minimising the risks associated with the current processes.[95]

2.75 In March 2009, DIAC provided a detailed schedule of work its Data Quality Team had undertaken since mid-2008 towards improving data quality. These take up many of the data quality issues raised by the ANAO during the course of the audit.

2.76 DIAC also reported that, despite its Data Quality Team's engagement with departmental data owners, action by those owners 'has been very slow' in

[91] Following the ANAO performance audit *Administration of the Health Requirement of the Migration Act 1958* in 2007, the Health Policy Section was seeking to strengthen the 'Health Undertaking' process.

[92] DIAC, internal minute, *CMAL Data Management Team—Data Quality Overview ARC06 – Health* (plus a series of other similar analyses), The CMAL team identified records potentially in need of attention by searching for selected words in the narratives (such as 'health cleared', 'cleared by MOC' and 'please delete'). After manual inspection, selected records were provided to Health Policy Section, who provided authorisation for deletion, as appropriate. The team noted that this is 'an *extremely* manual process' [emphasis in original].

[93] DIAC did not keep complete records of the numbers of deletions made from the start of this project.

[94] DIAC, internal minute, *CMAL Data Management Team—Data Quality Overview ARC06 – Health*. The Health Policy Section was also redrafting relevant parts of the PAM3 manual for health processing with a view to improving the instructions relating to MAL records.

[95] DIAC, email advice, Character Transition Taskforce Section, Compliance and Integrity Support Branch, 31 July 2008.

seven cases, there has been 'very little progress' in three others, and 'resistance to taking responsibility' reported in two cases. In one other case it was unable to identify a data owner.

2.77 The department has also advised that CMAL Operations Section's capacity to provide similar intensive assistance for other cases has been limited by the available resources and higher priorities.[96] DIAC also advised that the area responsible for running CMAL is planning to re-engage with Alert Reason owners, stating that 'Stakeholder Engagement [*is*] to follow in the successor [*group*] to the now closed CMAL Practice Management Group, to be convened in the first half of 2009.'[97]

2.78 A report on CMAL progress provided by DIAC during audit fieldwork notes that, due to CMAL system performance and the continued tether to HMAL, the data quality standards set out for CMAL cannot be met.[98] The report also notes that 'full CMAL rollout including SRS and the de-commissioning of HMAL will strengthen data quality.' However, it does not explain how.

(e) Data quality has declined in recent years

2.79 To compare data quality now with some point in the past requires a detailed account of how the data looked at a convenient previous time. The audit team identified a set of tests and results from the time of the Wheen Review which could form the basis of a comparison with July 2008 data.

2.80 The ANAO also analysed the PAL data to compare it with the value analysis done by DIAC's data mining project in 2006. In some cases, particularly non-*National Security* data, effective comparison was impracticable as the March 2006 data is incomplete. DIAC does not retain the original analysis and it is not possible to re-analyse the data from that time.[99]

[96] DIAC advice of 19 March 2009. Specifically, DIAC stated that its data management team is also a supporting team to the operations areas and, at times, particularly in the past 18 months of the CMAL deployment across all the visa, citizenship and border entry systems, it has been called upon to assist in sustaining operations at the expense of its core business. As a consequence, 'resourcing levels in the team to carry out that core business has not been ideal.'

[97] DIAC advice of 22 January 2009.

[98] DIAC, MAL Review Implementation—Project Sponsor Report, July 2008, p. 9.

[99] Detailed results are set out in Tables A.2 and A3, Appendix 2. DIAC did not perform a corresponding value analysis of the DAL part of the MAL database in 2006.

The Wheen Review analysed PAL records for completeness

2.81 The Wheen Review is the only earlier review of MAL that systematically analysed the data.[100] It stressed the need for accurate, current and complete records. It also assessed the completeness of PAL data (as of 27 November 2003), listing numbers of data deficient records by Alert Reason.[101]

2.82 When the audit tested the PAL data (18 July 2008) using the same tests as the review (save a redundant one)[102] it found:

- 19.9 per cent of PAL records were now data deficient, more than double the proportion—9.3 per cent—reported in November 2003;
- 27.4 per cent of high risk PAL records were data deficient, compared with 16.0 per cent in 2003; and
- setting aside *National Security* records, 10.2 per cent of records were now data deficient, up from 8.1 per cent in 2003.

2.83 By the Wheen Review's definition, most data deficient records are *National Security* records. On the other hand, by its nature, this is the category of record most likely to contain sparse information.

2.84 DIAC has advised that it has expended substantial resources on data quality management, aimed mainly at the high risk *National Security* component of the database, but not ignoring other high priority issues.[103] However, the above analysis shows that, despite these efforts, data quality has deteriorated for both *National Security* and non-*National Security* records compared with the position in 2003.

[100] Wheen Review, p. 57.

[101] The report of the Wheen Review shows only an analysis of PAL data. It did not analyse DAL data. The results of testing the 2008 data is set out in (see Table A.5, Appendix 2). This should be compared with the 2003 analysis of data deficient records in Table A.4, Appendix 2.

[102] The Wheen Review based its tests of data deficiency among MAL records upon nine specified tests, including the presence or absence of family name, given name, date-of-birth and so on and various combinations of such items. However, it became apparent during audit analysis that one of these tests is redundant: it identifies records also identified in other tests. Thus simply summing the numbers of data deficient records identified by the nine tests double-counts some records. This means that the proportion of data deficient records identified by the Wheen Review (12.6 per cent of PAL records) is too high: this should be 9.3 per cent.

[103] DIAC advice of 19 March 2009.

(f) DIAC has no effective quality assurance function on data quality

2.85 The Wheen Review emphasised the need for quality assurance of MAL entries for entries, updates, reviews and deletions. DIAC's Entry Operations Centre (EOC) staff have long been expected to 'provide an initial quality assurance service by ensuring RIF records meet the guidelines specified in [*the PAM3 manual*]'. However, the review concluded that 'the existing EOC check is not such a quality assurance process' and recommended 'a properly resourced quality assurance process be established to monitor and enhance the quality of data in MAL and that being entered into MAL.'[104]

2.86 To implement this recommendation, DIAC created the CMAL Data Management Team focusing on quality and reporting.[105] However, as noted earlier, although this team has done extensive work to identify data deficiencies, responsibility for quality lies with data owners, most of whom neither correct records nor quality assure them. No quality assurance function such as that envisaged by the Wheen Review and agreed and funded by government has been instituted.

(g) ANAO analysis found self-evidently deficient records

2.87 To test thoroughly whether MAL records are accurate and kept up-to-date requires access to source material to provide a basis for comparison. Opportunities to do this are limited. The ANAO's analysis identified the following problems:

(1) Dates outside plausible ranges.

(2) Internal inconsistency between related MAL records.

(3) Duplicate or near duplicate records.

(4) High-risk alerts with minimal biodata.

2.88 Each of these is considered briefly below.

(1) Dates outside plausible ranges.

2.89 The Sadleir Review found 27 people aged 97 or older listed on PAL for *National Security* or *Terrorism* reasons: the ANAO's analysis identified only

[104] Wheen Review, Recommendation 10.25.

[105] DIAC, MAL Review Implementation—Project Sponsor Report, July 2008, p. 9.

seven such cases.[106] However, it found a total of 1068 people on PAL aged 97 or more.[107] The likely reason is that the age-related data has been entered wrongly.

2.90 Similarly, the Sadleir Review found 117 people aged under 15 listed on PAL for *National Security* or *Terrorism* reasons. The ANAO's analysis identified 17 such cases among a total of 4880 records of people under 15 on PAL.[108]

2.91 Although the numbers of these records are small in comparison with the MAL database as a whole, these results still show that, ten years after the Sadleir Review pointed out the problem, dates in PAL records are not being checked adequately for plausibility.

(2) Internal inconsistency

2.92 Audit fieldwork identified a serious/high profile crime case for a sub-class 457 visa holder for whom, and for whose spouse, DIAC had entered records on MAL in July 2007. The husband's MAL record had been modified in December 2007 following the resolution of legal action before the courts. However, the narrative in his spouse's MAL record was not updated until May 2008. This latter update occurred only because the persons concerned, prominent non-citizens, had become the subject of 'current work on briefing the Minister [*which*] alerted [*Temporary Business Policy and Procedures Section*] to the discrepancy of the listings for these two individuals'.[109]

2.93 There is no easy way to identify any similar pairs of records in PAL. This case shows it is possible for such inconsistencies to exist. There is no known process for ensuring that when a PAL record gets updated, a related record for another person also gets updated where necessary.[110]

[106] Sadleir Review, p. 17, paragraph 51.

[107] Over four hundred of these have a birth date of 1900, which may indicate that the birth date is unknown.

[108] Some 1400 of these are listed for *Child Custody Concerns*, three were listed under *War Criminals*, 31 under *Serious Crime* and 89 as *Other Criminals*.

[109] DIAC, internal email from Temporary Business Policy and Procedures Section to Character Policy Section, National Office, 1 May 2008.

[110] DIAC has agreed that updating of related records is a 'real issue'. It suggested that 'for this and other reasons, CMAL requires a cross-reference field so that listings can be related to others in an obvious way' (advice of 22 January 2009). However, it has not advised whether any action is planned.

(3) The presence of duplicate or near-duplicate records

2.94 Testing the PAL database for records with duplicate bio data (Family Name, Given Name, Date-of-birth, Country-of-birth, Sex and Citizenship)[111] returned 3667 records which appear to be duplicates. This represents less then 0.5 per cent of PAL. Some of these records occur just once; that is, they represent a single duplicate of another record. Some occur several times; that is, there appear to be more than two records with identical bio data.[112] Multiple records were identical in every way except for the date-of-birth field. In each case, the records differed only in the year of birth shown.[113]

2.95 The majority of these cases are likely to be aliases of another record. DIAC business rules require such records to indicate a primary–secondary alias relationship. Addressing this will improve the efficiency of matching and processing. If DIAC does not address it, statistical reports may also record incorrectly the numbers of records in CMAL.

(4) High-risk cases with minimal biodata

2.96 In the light of DIAC's MDS and the value analysis set out above, the ANAO analysed selected examples of poor bio data in the PAL database. The analysis identified 243 cases with minimal bio data. Each of these records contained only a dash for *given name*. In each case, the entries in both the *country of birth* and *citizenship* fields are 'unknown'.

2.97 All these records meet DIAC's MDS for high risk records. However, with such poor bio data there is a risk that these records will return a large number of possible matches. DIAC may wish to consider the usefulness of these records if such poor bio data is likely to generate a match score that would be sufficiently high to warrant consideration.

[111] Testing verified first that there were no wholly duplicate records (which would require only the person number to be unique).

[112] These records had identical bio data in the fields mentioned above, but differed in other fields such as Person Number and Alert Number. Note: all known aliases were disregarded. The results reflect testing of records containing a blank Alias or marked as 'Primary'. Some records identified as duplicates were entered on the same date, others were not.

[113] In one particular example, similar records occur with a year of birth from 1965 to 1980 with various month and day combinations.

Conclusion—completeness and quality of MAL records

2.98 DIAC has a clear idea of the items of the data it needs to be in MAL to enable the department to undertake the matching task at the heart of MAL operations. Reviews have repeatedly warned, and DIAC has also long been aware, that many records are incomplete and that there are good reasons for the department to make its MAL records as complete as practicable.

2.99 An essential control to ensure completeness of MAL records is the data entry system. The introduction of the RIF brought some discipline to MAL data entry and the Wheen Review advocated its widespread use. However, it became apparent to DIAC that the original RIF was not adequate and still allowed entry of poor quality data.

2.100 Although DIAC has analysed its own data to identify deficiencies and improve quality, it has made limited progress in correcting these deficiencies. Many records in PAL—and a large proportion of new entries—have been entered for *National Security* reasons. Even though DIAC has worked with external security agencies to control and improve the quality of these entries, their overall quality is lower than in 2003. The proportion of non-*National Security* PAL records which are data deficient has also increased since 2003. Testing of specific fields revealed some other aspects that warrant attention by DIAC.

2.101 To make substantial progress with improving the completeness of MAL records, DIAC needs to address two problems: improving the quality of new entries and improving the quality of the existing stock of records. This could require DIAC:

(i) to progress, in a timely manner, the introduction of a new data entry mechanism which will give it the opportunity to introduce greater rigour to entered data (through edit checks and the like); and

(ii) to identify responsibility for ownership and hence, accountability and responsibility for existing records. However, it is not clear that the implications of formal data ownership are fully accepted by the identified Alert Reason owners.

2.102 In March 2009, DIAC introduced a new RIF facility, CMAL RIF (see para. 2.63 above). It advised that:

> The CMAL Remote Input Function (RIF) now incorporates additional checks on the expiry date of records with respect to their alert reason codes and some additional validation on birth dates. RIF processing responsibility has passed from the EOC to CMAL Operations. The longer term plan will be to give 24 x 7 support to airports and posts with the bulk of onshore requests being processed on the day shift. Further data quality improvements have been scheduled for SfP Release 10, in November 2009, where decommissioning of the Heritage MAL RIF will be completed.[114]

(3) Reviewing MAL records

The importance of reviewing and deleting MAL records

2.103 MAL records are unlikely to be useful in perpetuity. The person about whom a PAL record exists may no longer have the characteristics that warranted the record's inclusion in PAL. A document that formed a basis for a DAL record might simply no longer exist. DIAC therefore needs to erase or archive records promptly when they cease to be useful. Otherwise, they could:

- increase processing time as the MAL system attempts to match against such records;
- consume resources wastefully where possible matches are generated which, ultimately, are pointless; and
- cause inconvenience to travellers where such a match is actioned.

2.104 An internal minute notes: 'Failure to remove [*inappropriate entries*] from MAL … will result in years of potential inconvenience for a client, as well as creating unnecessary work for DIAC and, in particular, Airport staff.'[115]

2.105 To examine whether DIAC reviews and deletes MAL records effectively, the ANAO considered:

[114] DIAC advice of 6 May 2009.

[115] DIAC, internal minute, 'Commentary on Proposal for Health Undertaking Clients to be placed on MAL', 20 May 2008.

(a) whether DIAC has developed a systematic approach to reviewing and deleting unnecessary MAL records;

(b) whether DIAC has followed its business rules for reviewing and deleting MAL records;

(c) whether DIAC has been aware of the status of reviewing MAL records for some time; and

(d) the fact that testing shows outdated MAL records can easily be found.

(a) DIAC has designed a systematic way to review MAL records

2.106 DIAC could identify records for deletion either by ad hoc or systematic means. Ad hoc opportunities arise when updated information about a person on PAL becomes available. For example, if DIAC can gain assurance that a person has repaid their debt to the Commonwealth, and that was the only reason for them being on PAL, then the record can be deleted.[116] However, given that it is desirable to cull the MAL database of records that are no longer of value, a systematic approach is also called for.

2.107 A useful way adopted by DIAC, of systematically identifying records that no longer have value, is to include a review or deletion date when they are first entered into the system. DIAC has set out business rules in its PAM3 manual. This explains that a review code indicates the period the record is to remain on PAL, and whether it can be archived without human intervention.

2.108 The review/deletion date is set according to the reason for the entry, the Alert Reason.[117] That, in turn, requires that DIAC first identify a period for which it will ordinarily retain a MAL record before reviewing or deleting it. DIAC calculates some PAL review dates on the age of the person and others from the date of record creation. They vary from one month to 120 years, with

[116] Another technique to identify outdated records in the database would be to search for records that warrant scrutiny based on keywords in the narrative. This could be a laborious technique with limited prospects. However, a number of such records came to light during audit fieldwork and these are discussed later.

[117] 'Review' implies a requirement for manual consideration and judgment before deletion.

higher risk categories attracting longer retention periods. DIAC has legal advice that it has discretion to set the review period as a matter of policy.[118]

2.109 Setting the review code is not automatic, even though DIAC policy requires it to be consistent with the Alert Reason. Instead, the officer who first enters the record must enter the review code—a combination of the date at which the record is to be reviewed or deleted and an indication of which of those actions should be carried out (review or deletion).[119]

2.110 DAL records also contain a review code. The review or deletion date varies according to the expiry date of the travel document, or ten years after the creation date of the document.

(b) Whether DIAC adheres to its business rules for review of MAL records

2.111 In the light of the above, the ANAO examined MAL records to identify:

(1) whether all records had been assigned a review date and code;

(2) whether dates were assigned consistent with DIAC business rules; and

(3) whether review dates were now being adhered to.

Presence and distribution of review dates

2.112 Testing found that all MAL records except two had been assigned a review date and code.[120] To get a general perspective on the duration of MAL records the ANAO examined the distribution of review periods throughout the database. This shows the intended 'shelf-life' of each record at the time the record was entered (calculated by subtracting the review date set from the date the record was entered).

[118] Advice received by DIAC, 30 April 2008. Note: It is not clear if DIAC has obtained the concurrence of the Director-General of the Archives to a determination being made that MAL records that remain active for more than 25 years not be required to be transferred to the Archives under s. 27 of the *Archives Act 1983*.

[119] They are required to do this according to the rules set out in the PAM3 manual. The rules include a requirement for inclusion of a code—either 'R' for 'review or 'D' for 'delete'—indicating what action will take place when the specified date is reached. DIAC intends that review cases be examined by staff before taking a decision to retain or delete them. Cases marked 'D' are to be automatically deleted without human intervention at the end of the month of the deletion date

[120] The ANAO identified two records, both in DAL, which did not have a review date. After these were brought to DIAC's attention it advised that it had deleted them.

2.113 This testing shows that a large proportion of MAL records are compliant with the review periods set. However, there are 619 MAL records (including 586 PAL records) with an original validity period of greater than 120 years. This is outside any existing stated review period in DIAC policy (See Table 2.1). These records clearly require attention.

Table 2.1

Original 'life' of MAL records, based on review periods set

Actual review period in years	PAL	DAL	Total	Percentage of MAL
0–10	89 932	2 197 225	2 287 157	74.54
11–25	42 116	182 726	224 842	7.32
26–50	303 597	189	303 786	9.90
51–75	212 326	154	212 480	6.93
76–100	38 078	480	38 558	1.26
101–120	736	65	801	0.03
121+	586	33	619	0.02
Total	**687 371**	**2 380 872**	**3 068 243**	**100.00**

Source: Results of ANAO testing of MAL database, dated 18 July 2008.

Consistent application of business rules

2.114 The ANAO compared the review periods set in MAL records and the relevant periods specified in DIAC policy.[121] Some review periods are based on the elapsed time from the date of creation of the record and others on the age of the person. Errors in these items can affect the calculation of the review date.

2.115 Nearly 57 000 PAL records have excessive review periods. A further 88 000 PAL records have review periods less than required. Overall, some 22.31 per cent of records (excluding *Debts to the Commonwealth* cases) have an incorrect review period.[122]

[121] For some Alert Reasons, there is more than one standard review period according to the sub-category of case under consideration. For example, an *Immigration Malpractice* case can attract either of two review periods according to the nature of the malpractice.

[122] Table A.6, Appendix 2, shows, by Alert Reason: the review period(s) set out in the PAM3 manual; the numbers of records with a review period less than prescribed; same as prescribed; and longer than prescribed. Note that records for *Debts to the Commonwealth* could not be analysed for this variable.

2.116 Care must be taken in interpreting this analysis. Although each case indicates an error in a MAL record, in some cases the error lies in the record of the person's date-of-birth, rather than (or as well as) the review date.[123]

2.117 A related matter is that DIAC has changed its business rules over time. For example, it has increased the review period for *Health Concerns*, from the person reaching 100 years of age to 120. Most records in this category—56 204—show a review period of 100 years. DIAC has not changed the review period of existing records after varying the standard. This could lead to inconsistent handling of otherwise similar cases.

2.118 In DAL, there are 183 647 records (some 7.71 per cent) set at greater than the required review period of up to 10 years from creation.[124]

MAL contains records past their review date

2.119 Most MAL records (92 per cent of PAL and 99 per cent of DAL) are marked for automatic deletion in due course. That is, they will be deleted by the system without human consideration or intervention. All others (8 per cent of PAL and 1 per cent of DAL) are marked for review, meaning a DIAC officer will decide at the time of review whether to delete or retain the record. Any record which is due for review but passes its review date remains active on the system until the review is carried out.

2.120 Testing found that MAL contains 5752 records (5643 PAL and 109 DAL) which had passed their review date, as of 18 July 2008. Most of them should have been reviewed more than 18 months ago. Of the 5643 overdue PAL records, some 96 per cent are *War Crimes* cases (See Table 2.2).

[123] Listed in MAL for the Alert Reason *Serious or High Profile Crime* are eight records with a '0' in the date-of-birth field, and six records with a year of birth of 1865, suggesting the person of interest is currently aged 143. The review date on these six records is in the year 2100, when the person will be aged 235. In this case '1965' may have been intended for '1865'.

[124] The ANAO advised DIAC of the DAL records with apparently excessive review dates. The nature of the error is sometimes apparent. For example, the ANAO examined three records with a review date some six hundred years hence. All three were entered on 26 November 2007. The review date appears as '261112', which the person entering the data may have intended as '26 November 2012'—exactly five years from the date of entry—but which is interpreted by MAL as 'December 2611'. The ANAO found numerous examples similar to these.

Table 2.2

When current overdue records should have been reviewed

Review Year	PAL	DAL	Total
0	0	2	2[125]
2005	2 049	0	2 049
2006	1 716	0	1 716
2007	1 860	1	1 861
2008	18	106	124
Total	**5 643**	**109**	**5 752**

Source: ANAO analysis of MAL database

(c) DIAC has been aware of the status of reviewing MAL records

2.121 The Wheen Review criticised how DIAC reviewed MAL records:

> 'Review' is largely a misnomer as overwhelmingly records are deleted without a Review, i.e. no quality control check is made by EOC on the Review date. This is contrary to the original intention of a quality control check before such action, but this has largely fallen into disuse because of the substantial increase in the volume of work EOC had, including associated with MAL ... Further, experience of recent years has been that a Review date generally meant that the officers who were the 'owners' of particular data and had individual records referred to them were too busy or otherwise not inclined to give substantive consideration to the records and therefore just rolled them over.[126]

2.122 Three years later, the CMAL Data Analysis team concluded 'data quality is currently very poor in MAL due to the fact all user[s] have the ability to enter any review code and date without the system providing [any] warning or error messages.[127]

2.123 At the same time, a DIAC Internal Database Analysis review identified 4120 PAL records that were then past their review date. These were all originally set for review between August 2005 and December 2006.[128] The DIAC analysis attributed the lack of review to a 'major breakdown in com-

[125] DIAC has stated that these two records have now been deleted.

[126] Wheen Review, Appendix B2, 'Deliverable B2 et al.'

[127] DIAC, 'Useability concerns and requests for amendments', 12 January 2007.

[128] DIAC, IDA – Overdue MAL records for review, circa December 2006.

munication between MAL and the individual stakeholders' and stated that this, together with a failure to adhere to PAM3 manual, showed a need for immediate corrective action. This review 'strongly recommended that relevant stakeholders be strongly encouraged to participate and take ownership of all aspects of the Alert Reason, for which they are the true data owners.' It addressed the need for responsibility for data be taken and adherence to DIAC policy be achieved before CMAL started.

2.124 The ANAO re-analysed the data intended for review in the August 2005 – December 2006 period in the July 2008 database and found 3765 active records, suggesting that in the interim, DIAC had deleted only 8.62 per cent of the records that its analysis had found to be overdue eighteen months earlier. The full comparison is in Table 2.3.

Table 2.3

PAL overdue records: comparison at two dates

	Numbers of records overdue at ...	
Intended review date[129]	31 December 2006	18 July 2008
August 2005	880	821
September 2005	17	14
November 2005	1 346	1 198
December 2005	18	16
July 2006	13	13
August 2006	212	204
September 2006	281	244
October 2006	356	322
November 2006	285	257
December 2006	712	676
Total	**4 120**	**3 765**

Source: DIAC and ANAO analyses of MAL database

Procedures for review and deletion

2.125 It is one thing to set a review period in the MAL record: it is another to ensure that a trigger causes a review to happen at the right time. Currently reviews are instigated manually. A CMAL Operations officer must generate a list of records that have reached their review date by finding them in MAL.

[129] Not every month over this period is included here as some months did not have any review periods set to expire in those months.

2.126 DIAC advises that its Border Operations Centre (BOC) assesses records with low-risk Alert Reasons that have reached their review date. High risk cases are referred—by email—to the relevant Alert Reason owner. A DIAC medium-risk Alert Reason owner offered a contrary view, stating that 'we do not receive reports although it would make removing outdated MAL listings ... easier.'[130]

2.127 DIAC advises that 'dialogue continues between the stakeholders and the CMAL Data Management team. The PAM3 [*manual*] provides for CMAL [*Operations*] to take the lead where a stalemate or unresolved matter prevails.'[131]

(d) Whether outdated records can easily be found in MAL

2.128 It is possible to find (by searching for keywords in narratives and by inspection) some records that are manifestly out-of-date. This report considered the presence of records of *Health Concerns* cases whose narratives contain instructions like 'Please delete' earlier (see paragraph 2.72). Other instances encountered are set out below. These cases show that, even if the existing business rules for review and deletion were rigorously observed, additional processes for removing outdated records would improve the MAL database.

2.129 The ANAO found 39 records in PAL where the narrative stated that the person was dead. The following three instances are typical:

> Client is deceased as of [date].
>
> INTERPOL cancellation notice [number] [code] – deceased.
>
> Confirmation received that client is deceased. Death certificate attached to file.

2.130 Equally anomalous is a record created in 2007 listed against *Health Concerns,* whose narrative states: 'Health issue addressed—death cert[*ificate*] sighted.' These four examples were still active on the system in July 2008 and due for review in the years 2056, 2081, 2065 and 2055, respectively.

[130] DIAC email to ANAO, 22 May 2008.

[131] DIAC advice of 22 January 2009.

Case study: Myra Hindley

Myra Hindley (born 23 July 1942) was convicted of killing two children in Britain between 1963 and 1965. She was sentenced to life imprisonment in 1966. She died in November 2002. The case was infamous and her death widely reported in Australia at the time.[132]

PAL records were created for Hindley in 1985: a primary record under her own name plus two aliases, 'Myra Spencer' and 'Clare Stewart', names which MAL alleges Hindley used.

All records endure on the July 2008 copy of MAL examined by the ANAO although Hindley had died some five years earlier.

Further, each record also includes an update of 26 March 2008. This states: 'LONDON [*post*] ADV[*ises that*] [*a similar name to one of Hindley's aliases*] [*born*] [*specified date*] N/S [*is not the same person*].PL S [*sic*] ALLOW ENTRY [*to the latter*].'

This amendment must have derived from a visa applicant or traveller being wrongly identified as a potential match to a MAL record for a Hindley alias. DIAC—even at its London post—does not appear to have been aware of Hindley's death. Removal of the records for Hindley would obviate such mismatches.

In the July 2008 copy of MAL, the three records for Hindley had been set for review in July 2042.

This illustrates that records of deceased persons have the potential to remain on MAL for many years and to generate mismatches.

DIAC advised in January 2009 that it had now deleted these records.

2.131 DIAC derived MAL records for American serious criminals from the US Marshals' web site in 2000.[133] The website shows that one of the criminals listed had been shot dead in August 2003 and a further three had been captured over the intervening years: yet, as of July 2008, their MAL records endure. The record for the criminal shot dead in 2003 is set for review in 2063 and the others at various times from 2046 to 2077.

2.132 DIAC points out that there is:

[132] See, for example, *Sun Herald*. Sydney, 17 November 2002; *Sunday Telegraph*, 17 November 2002; *Australian*, 18 November 2002.

[133] The narratives show the Internet address. See: <http://www.usdoj.gov/marshals/> [accessed 7 May 2009].

> no effective way of being apprised of [*the demise of listed persons*] in the case of all records on PAL, and it is beyond the resources of the department to carry out extensive fact-of-demise type investigations.[134]

2.133 However, allowing records representing identities of deceased people to accumulate in MAL has other costs, in processing effort and unproductive checking. The challenge for the management of MAL is to determine and apply a cost-effective level of resources to removing such records.

Conclusion—reviewing MAL records

2.134 ANAO analysis shows that there are a range of deficiencies in the quality of the MAL database, all of which could be addressed by improvements in DIAC's approach to MAL's maintenance. In some cases, the required action is apparent. For example, a system needs to be instituted to ensure that MAL records attract the review period appropriate to their Alert Reason. This could be done through automated means in a revised data entry system.

2.135 Other corrective action is more complex and the required procedures not so apparent. For example, it may be difficult to identify some of the records within the system where the nominated person has died. Certain examples observed by the ANAO were detected by inspection rather than directed search. As the size of the MAL database increases it is an ever more challenging prospect to seek such records and delete them. It may seem an unprofitable practice. However, against this must be weighed the risk that redundant records will cause unnecessary matches, generate fruitless work and inconvenience innocent parties.

Conclusion—the completeness, quality and currency of MAL data is an enduring problem for DIAC

2.136 Earlier reviews of MAL have identified persistent shortcomings in the management of MAL data: in collecting all the right records, in maintaining data quality and in deleting outdated information. Audit analysis showed that these shortcomings endure. This could lead to:

- failure to identify a person who poses a threat to the community if they are not on the list when DIAC checks and a consequent risk of admitting such a person;

[134] DIAC advice of 19 March 2009.

- inefficient processing where information is incomplete or out-of-date;
- vigilance fatigue among MAL staff; and
- some loss of confidence in the MAL system as a whole.

2.137 Regardless of the particular data quality issue, DIAC needs to resolve who is responsible for the integrity of its MAL data. This is both a persistent and strategic issue. Currently, much depends on the soundness of the original data entry by any of several thousand staff. There has been no substantial edit-checking at data entry to ensure the quality of the information that is entered.

2.138 Records are entered into MAL for any of a variety of 'Alert Reasons', reflecting the specific interests of DIAC 'Alert Reason owners' in diverse parts of the department and from external agencies. However, most DIAC Alert Reason owners, though regarded as 'data owners', have not assumed full responsibility for the data. This is because the data is and can be entered by many officers throughout DIAC and externally, action over which DIAC Alert Reason owners have no control.

2.139 DIAC has put the view that management of data quality is a priority for DIAC, but 'it is largely an issue of effectiveness rather than efficiency' and it ranks the issue behind the actual performance of MAL checking and loading additional *National Security* records. DIAC has also stated that:

> it is in the nature of alert lists that some of the information provided on individual identities and sources will be incomplete, and proper risk management will cause the managing authority to err on the side of caution.[135]

2.140 However, the records that DIAC itself enters relate to its own clients, on whom it generally holds more complete data. Further, some of the deficiencies identified in this chapter flow not from gaps in original data sources but from inconsistent application of departmental business rules (such as setting dates for review of records).

2.141 DIAC is well aware of the deficiencies in its own MAL data. It has carried out regular reviews with the intention of identifying and, ultimately, correcting such deficiencies. Most often, these actions falter at the point where someone within DIAC has to take responsibility for carrying out corrective

[135] DIAC advice of 19 March 2009.

action. The issue of data ownership has long been identified but it clearly requires firm management decision and action to address it.

2.142 Several streams of action are needed to deal with both the stock and the flow of data:

(1) *Develop a plan*—A foundation step would be the development of a plan for the population and maintenance of the MAL database. This plan would identify:

- roles and responsibilities of all parties involved, particularly the data custodians and CMAL operations area;
- the data quality matters that need to be addressed and the rules that will be adopted to ensure that the data entered is fit for purpose having regard to risk involved;
- how the responsibilities and rules will be codified and documented. This may involve memoranda of understanding (MOUs) where external agencies are involved and memoranda of arrangements for internal DIAC functional units;
- how the arrangements will be reviewed and monitored to ensure they are working well.

(2) *Improve new data*—This would lead to the flow of new data into the system being better controlled by data entry arrangements that ensure appropriate standards—reflecting DIAC's business rules—on the data being entered are observed. Such arrangements should be capable of implementation once CMAL is settled in full operation and vestiges of the previous version of MAL (now called 'Heritage MAL') shut down.

(3) *Review existing data*—At the same time, the stock of existing MAL records would need to be addressed. DIAC has done numerous analyses of the problems in these records but without any follow-up action to correct them. Regular reviews of progress in cleaning the MAL database would help to ensure work proceeds satisfactorily.

Recommendation No.1

2.143 The ANAO recommends that DIAC develop a plan for the population, maintenance and review of the MAL database. This should include, at a minimum:

- clarification as to who (within the department and externally, as appropriate) is responsible for MAL data, the quality issues to be addressed and business rules for addressing them; and
- a course of action which includes:
  - arrangements for data entry into MAL that ensures its own business rules and desired quality standards are observed;
  - instigation of a program, with target dates, for data cleansing its existing stock of MAL records; and
  - a mechanism for reviewing and reporting progress with this work.

DIAC response: *Agreed*

DIAC agrees to develop a plan as recommended, including a mechanism for reviewing and reporting progress. We will review and clarify current arrangements for MAL data and data quality responsibility. We already have an ongoing program of data quality checks and improvements and we will continue to undertake a range of actions designed to improve data quality within the MAL database. Priority will continue to be given to the focus on high risk records, in particular working with security agencies to improve data quality in the national security component of the database.

In developing arrangements for data entry that ensures observance of business rules and quality standards, DIAC does not consider that the minimum data standards for MAL entry should be made mandatory, in all situations, either at the point of data entry or after a fixed period for review. DIAC considers that the greater risk in MAL operations lies in erecting barriers to the entry or retention of records in the PAL which can provide valuable advice to decision-makers and alerts to external stakeholders such as security agencies.

3. Controlling access to MAL

This chapter examines how DIAC has controlled access to MAL to limit opportunities for inappropriate browsing and inadvertent or malevolent data entry.

Why DIAC must control access to MAL

3.1 Some 4026 officers, mainly DIAC staff in Australia and at overseas posts, plus a few external agency officers, have access at various levels to MAL.[136] The database is classified and those allowed access must be cleared. The PAM3 manual states that officers must access MAL only on a need-to-know basis:

> Access must be limited to DIAC work and under no circumstances should it be used for personal reasons. Any person who discloses MAL data without authorisation may be prosecuted under the *Crimes Act 1914*.[137]

3.2 Different levels of access are available, according to the user's responsibilities. For example, sensitive details (such as narratives in high-risk cases) are not generally visible to some users.

3.3 Controlling access to a system that has such a large number of users requires detailed procedures and continuous effort. To test DIAC's controls on access to MAL the ANAO considered:

(a) DIAC's controls on the number of people with access to MAL;

(b) DIAC's use of an audit trail for MAL transactions;

(c) DIAC's controls on the entry of inappropriate records; and

(d) DIAC's auditing of unnecessary browsing of MAL and other records.

(a) Improved controls have recently been put in place

3.4 DIAC has shown that it did devise a set of arrangements for the control of access to MAL by providing a copy of a manual, intended as guidance to the CMAL team in controlling the access of DIAC and selected external officers.[138]

[136] DIAC advised (22 January 2009) that, as of 7 November 2008, there were: 4045 users on MAL; 4026 had 'active MAL status'; 3067 users had RIF access; 19 users had been terminated/suspended; 897 new users had been added in the previous 12 months.

[137] PAM3 manual, p. 78.

[138] DIAC, 'Movement Alert MAL Access Handbook', May 2007.

This manual shows that MAL access, when granted, is time limited from three months to three years.

3.5 DIAC's CMAL Data Management Team reviewed MAL access in early 2007 and made recommendations for improvement. In October 2007, following the DIAC internal *Onshore Assurance Review 2006–07*, which recommends regular review of MAL access, the Data Management Team planned a cycle of reviews every 90 days to ensure each user has a continued business need to access MAL.

3.6 The regular 90 day cycle began in March 2008, shortly before the ANAO's analysis began. A message was circulated with a list of 45 DIAC officers with various levels of MAL access who had not used that access 'for a while'. The message apologised for the backlog in the review process but added that it had been 'a while' since a check of this sort had been done.

3.7 It is evident that DIAC is now seeking to control access to MAL in a systematic way, though its earlier efforts were less active. DIAC advises that this process continues on a 90-day cycle, as originally intended in 2007.[139]

(b) DIAC has an audit trail for MAL transactions but does no systematic analysis

3.8 DIAC demonstrated to the ANAO a robust audit trail for MAL transactions. It advised that 'all add/change/delete data is retained ... indefinitely.'[140] Where room for display of narratives [*in MAL*] is exceeded, overwritten text is retained in retrievable archives. BOC staff can identify who is responsible for each change by the logon ID of the user, which is recorded against the change. DIAC's training courses on the use of MAL include advice about the audit trail and that changes can be traced to the officer responsible.

3.9 There is no systematic review of changes made to MAL, however. Only where transactions come to the EOC for entering into MAL is there an opportunity for them to be reviewed. Otherwise, CMAL Operations Section believes that it is highly likely to come across any misguided/inappropriate transactions in the ordinary course of business.[141] The onus is on the officer

[139] DIAC advice of 22 January 2009.

[140] DIAC, email advice, 29 May 2008.

[141] DIAC, email advice, 29 May 2008.

who initiates a transaction to act properly, in accordance with APS values and code of conduct, and DIAC's policy instructions and security requirements.

3.10 DIAC advises that ad hoc analysis of the audit trail may be done by CMAL operators when investigating cases. Reasons may include identifying who updated a narrative incorrectly; who created the alert and when; who referred a likely match; and identifying those who may need further training.

3.11 DIAC also advises that, where any misuse is suspected, the BOC:

> deals directly with any person who is not using the system properly. Where the audit trail identifies a person who is not performing their work duties in accordance with procedures and guidelines, the officer is generally spoken to by their team leader to isolate the reason. In many cases it is minor for example not updating the MAL narrative and is corrected by additional training or coaching. If it is serious this will be dealt with at the higher level.[142]

3.12 DIAC provided no documentary evidence of having addressed any incorrect use of MAL data in the way it describes.

(c) DIAC has no control on the entry of inappropriate records

3.13 There is a risk, however remote, that someone among the officers with MAL access could seek to create a biased or vexatious record. DIAC advises:

> Quite simply it is possible for a user to enter malevolent information directly into MAL without it being picked up straightaway. The processes we have in place are: when there is a true match or likely match to the MAL alert and as per normal it is investigated prior to it being referred it will be picked up … The PAM3 document places the onus on the officer creating the record to act in accordance with policy and legislation. [143]

3.14 In other words, DIAC does not have any quality control on data entry—a check, either exhaustive or sample-based at the time of entry that the records are appropriate. Rather, it allows entries to be made without a check expecting to identify inappropriate records when a match occurs. This means that such a record could remain in MAL at least until it happens to yield a match.

3.15 The ANAO is not aware of any vexatious record having been created or having caused a nuisance to those inappropriately recorded. However, with no quality controls at entry there is only general staff awareness of the audit trail

[142] ibid.

[143] DIAC, email advice, 27 May 2008.

to inhibit entry of such records and no easy way of gaining assurance that none lies within the database.

(d) DIAC's auditing of unnecessary browsing of MAL and other records has been superficial

3.16 DIAC provided evidence that it could, and has, audited unnecessary browsing of records by departmental staff.[144] That evidence, in the form of a review by the department's Values and Conduct Section in 2007, involved accessing DIAC records on several major IT systems, including MAL, about two high-profile cases.[145] DIAC's evidence shows that it has, at least on this occasion, checked on staff viewing MAL records.

3.17 DIAC's internal review found that, of 112 DIAC employees who accessed these records on various systems only one employee did not have a legitimate business reason, but accessed the record out of curiosity. The system accessed by this employee was not MAL.

3.18 The Values and Conduct Section concluded that 70 of the 112 staff had a legitimate purpose in accessing the records on the basis of their 'business area title and role and the position title description of each staff member as indicated by the DIAC staff directory.'[146] It pursued the other 42 cases by individual follow-up.

3.19 DIAC advises that the Values and Conduct Section is 'hoping to become more proactive' in regard to such reviews. However, there is no documentation it can provide.

Conclusion—DIAC could improve controls over access to MAL

3.20 DIAC has a system in place to control who has access to MAL which, if it continues the active review process that it started in 2007, will allow it to maintain that control. Reviewing all MAL transactions would be resource-intensive but DIAC could address the lack of quality control over data entry by review of a risk-based sample of change/update transactions. These reviews could also be part of a generally improved system of quality control over MAL data entry.

[144] DIAC, email advice of 22 May 2008.

[145] The cases were those of Dr Mohamed Haneef and Mr Calvin Broadus, aka 'Snoop Dogg'.

[146] DIAC, email advice of 22 May 2008.

4. Australian citizens on MAL

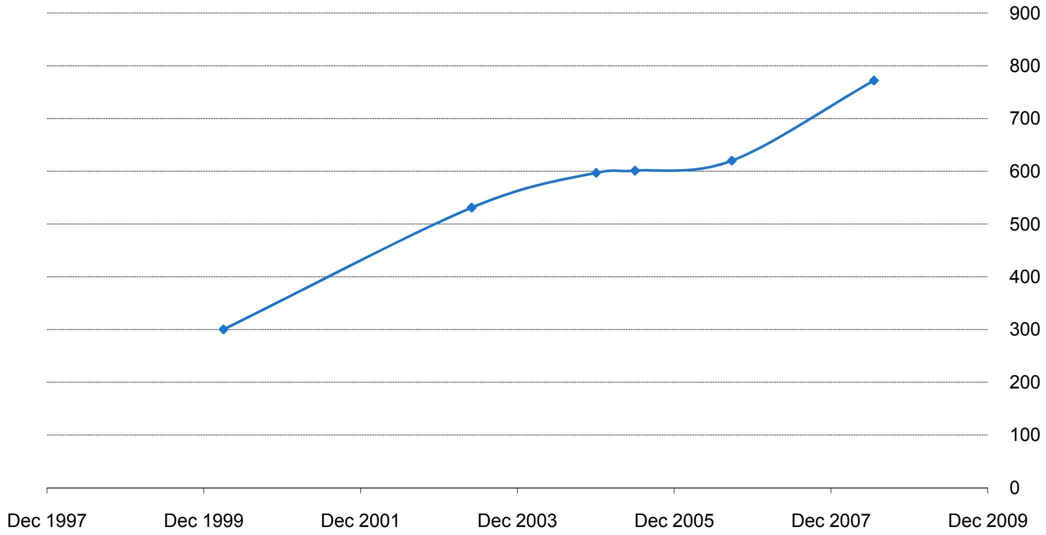
This chapter considers the DIAC practice of including some Australian citizens on PAL and assesses the nature of its controls on this practice.

Whether Australian citizens should be recorded on MAL

4.1 DIAC is responsible for 'entry, stay and departure arrangements for non-citizens'.[147] Its main legislation is the *Migration Act 1958*, whose object (s. 4) is to regulate, in the national interest, the coming into, and presence in Australia of non-citizens. Consistent with this, the PAL part of MAL was meant to list non-citizens of concern.[148] Since 1998, DIAC has listed increasing numbers of records on PAL for Australian citizens, though they are few in comparison with non-citizens. In July 2008, there were over 700 such records.

Figure 4.1

The number of PAL records identified as Australian citizens has grown



Sources: DIAC documents and ANAO analysis of the MAL database.

[147] Administrative Arrangements Order, 25 January 2008.

[148] DIAC, Gerlach Review, 2000, p. 21.

4.2 DIAC advised that:

> No agency, DIAC included, is capable of exercising a power to prevent Australians from returning to Australia, and MAL listings play no part in the processes—passport cancellation in particular—that can prevent an Australian from travelling overseas.[149]

4.3 The ANAO considered:

- DIAC's practice in recording Australians on MAL, examining PAL in particular;
- DIAC's current business rules, including what legal support it has obtained; and
- what records of Australians are actually on PAL.

DIAC's practice and how it has developed

4.4 DIAC originally recorded only non-citizens on MAL. Where Commonwealth authorities wanted to be alerted to an Australian crossing the border that would be recorded in the former Customs and Border Protection system, PASS, and its successor, PACE.[150]

4.5 In May 1998, DIAC reassessed its practice because of an increase in the number of Australians involved in immigration malpractice, such as people smuggling. The then MAL Interdepartmental Working Group endorsed listing Australians involved in people smuggling on MAL, for six months (or until interdiction occurred).[151] Authority to list Australians was restricted.

4.6 In 2000, the Gerlach Review found listing Australians on MAL had 'evolved without formal policy being set' and that 'referring Australians on arrival at airports may be legally problematic'. It recommended that DIAC 'develop policy regarding the circumstances under which Australians can be placed on MAL.'[152] There is no evidence of action on this recommendation.

[149] DIAC advice of 19 March 2009.

[150] This is consistent with the view taken by the Sadleir Review (1998). It is also consistent with advice given to Parliament by the then Attorney-General in November 2003 (Hansard, House of Representatives, 4 November 2003, p. 21 928). PACE is being superseded by a newer system called 'EPAC'.

[151] Wheen Review, Appendix 2, 'Inclusion of Australian citizens on MAL'.

[152] DIAC, Gerlach Review, pp. 5, 12 and 21.

DIAC obtained legal advice in 2002 about Australians on MAL

4.7 The above arrangements remained in place for about four years.[153] In September 2002, DIAC sought specific legal advice on its then practice of listing Australians involved in organised immigration malpractice and people smuggling. The section responsible for MAL summarised the legal advice:

> 1. We need to have strong grounds for listing an Australian citizen on MAL—i.e., previous convictions for immigration malpractice or objective evidence that the person may be involved in such activities.
> 2. It is important to note that [DIAC] has no authority to delay or question Australian citizens otherwise than with their consent.
> 3. Any suspicions by a [DIAC] Officer leading to a MAL listing have to be reasonable, not just subjective.
> 4. If an Australian citizen passenger is delayed unreasonably, the Department may face litigation based on the law of tort.[154]

Wheen Review

4.8 Advice on whether Australians should be listed on MAL was a specific deliverable for the Wheen Review.[155] At the review's outset, in June 2003, there were 531 Australian citizens on PAL, of whom 327 (62 per cent) were listed for *Organised Immigration Malpractice*.

4.9 The review team found that Intelligence Analysis Section (IAS), responsible for approving all Australians listed under *Organised Immigration Malpractice*, was reviewing all such records:

> They have reviewed some one third of the entries and identified about one third of these records as ones which should be deleted because they refer to circumstances no longer relevant.
>
> IAS has no operating instructions or procedures as to criteria for inclusion of Australians. When consulted by officers elsewhere in the Department they make decisions on the apparent usefulness of placing such an entry on PAL in relation to combating immigration malpractice. They advised that they are

[153] Email from Assistant Director, MAL, 5 February 2002.

[154] Email from Assistant Director, Movement Alert List, Entry Systems & Movement Alert Section, to various others within DIAC, with AGS advice attached, 18 October 2002.

[155] Wheen Review, Appendix 2. Later evidence shows that the Review did not consider the issue of Australian citizens listed on MAL for reasons of *National Security*. See DIAC, internal minute 'Australian Citizens Listed on MAL', 19 July 2005.

> significantly influenced by wanting to have an alert on movements of people across the border.

4.10 In December 2003, during the review, the MAL Review Steering Committee considered advice on this topic.[156] It agreed to a range of recommendations including that 'IAS complete the cull of [*organised immigration malpractice*] records of Australians as soon as possible'.

4.11 The Wheen Review recommended:

> 16.17 Instructions be amended to enable the listing on MAL of Australian citizens who are suspected of having committed, or having been convicted of, immigration-related offences.
>
> 16.18 The Instructions to staff make explicit that Australian citizens matched against a MAL record should only be delayed and questioned where they consent to this ... The Instructions should give staff clear guidance as to the sorts of circumstances in which citizens may be intercepted at the border.
>
> 16.19 Relevant business rules and computer systems be updated to incorporate MAL checking (both PAL and DAL) for Australian citizens.

4.12 These recommendations formed part of the proposal that went to government and was approved and funded with the CMAL project, in April 2005.

Progress with Wheen Review recommendations

4.13 In July 2005, an internal DIAC report[157] on progress with implementing the above recommendations found that:

> In January 2005 there were 597 Australian citizens listed on MAL which is an increase from 531 listed in June 2003. The majority are still [*Organised Immigration Malpractice*] alerts. After analysis of the alerts it was apparent that most had been listed for a long time without being updated. *At face value it would be reasonable to assume that a significant proportion may no longer be relevant.* [Emphasis added].

4.14 As a first step in reviewing records of Australians on MAL, DIAC gave Alert Reason owners a printout of 'their' records. Although the expectation

[156] DIAC, MAL Review Steering Committee, minutes of meeting, 18 December 2003.

[157] DIAC, Border Security Liaison Section, internal minute, 'Australian Citizens on MAL', 19 July 2005. The recommendations considered include those agreed by the MAL Review Steering Committee on 18 December 2003 (see para. 4.8) as well as those endorsed by government (para. 4.11).

was that unwanted records would be culled, the report shows a subsequent slight increase in the number of Australians on MAL (from 597 to 601). It further reports that IAS had deleted none of the records listed for *Organised Immigration Malpractice*. Other data owners had deleted very few. It goes on to say:

> Despite MAL being our principal electronic alert list and data quality having a direct impact on its effectiveness and Australian Citizens being possibly unlawfully listed on MAL, there seems to be little priority being given to cleansing the Australian Citizen records on MAL. It should also be noted that what data owners are being asked to do has been agreed to by the Executive.

4.15 The report concludes by recommending a range of actions to 'audit', review, update and delete records of Australian citizens on MAL. It is not clear why the reviewing and culling action—including that specifically directed by the MAL Review Steering Committee—had not been done.

DIAC's instructions about recording Australians on PAL

4.16 Current DIAC instructions state that the listing of Australian citizens on PAL requires clearance and may be for any of three reasons:[158]

(1) for *National Security* reasons. Clearance must be provided by the BOC;

(2) if they are suspected of or have committed *Organised Immigration Malpractice*. In these cases, IAS must clear the proposed listing; or

(3) if their *Australian travel document is damaged* or in poor condition.

4.17 In addition, the instructions add: 'where it is thought appropriate [*by the DIAC officer wishing to enter information onto MAL*] to list an Australian citizen on MAL for other reasons the record must be approved by CMAL Operations.' This suggests that sound reasons exist beyond the three mentioned above. The instructions provide no indication as to what these may be.

[158] DIAC, PAM3 (Policy Advice Manual), GenGuide A—MAL (Movement Alert List)—Policy & procedures, 1 December 2007, pp. 49–50.

Contents of the narrative

4.18 Reflecting the legal advice DIAC obtained in 2002 and one of the Wheen Review recommendations, its instructions also require all immigration-related listings to include in the narrative of the record that:

> the citizen's co-operation is requested in relation to clarifying the matter. DIAC officers have no authority to delay or question Australian citizens in immigration clearance without their consent.[159]

Legal basis for these instructions

4.19 As discussed earlier (para. 4.7), DIAC obtained legal advice in 2002 that supports listing Australian citizens for immigration malpractice. The DIAC instructions explain that the *Australian Passport Act 2005* provides a basis for considering any Australian travel document that is damaged to be invalid. They also explain that the purpose of listing is to give the Department of Foreign Affairs and Trade an opportunity to examine the document.[160]

4.20 The PAM3 manual states that 'Australian citizens may be listed for national security reasons'.[161] However, the ANAO is unaware of any legal basis for listing Australian citizens on MAL for national security or any reason other than immigration malpractice. In the absence of a purpose that relates to DIAC's functions or an exemption from the provisions of the Privacy Act, these entries may be problematic.

Analysis of records of Australian citizens on PAL

4.21 Audit analysis of PAL records shows why Australian citizens are listed there by primary Alert Reason (see Table 4.1). The ANAO compared these results with a similar analysis by DIAC from late 2006.[162]

[159] ibid.

[160] DIAC advised that no formal memorandum of understanding between departments appears to exist covering this arrangement (DIAC advice of 16 February 2009).

[161] DIAC, PAM3, GenGuideA—MAL (Movement Alert List)—Policy & procedures, s. 19.7.

[162] DIAC, *Internal Audit Report*, Border Security Division, Border Security Systems Branch, CMAL Data Analysis Team, undated but estimated circa October 2006.

Table 4.1

Australian citizens on PAL: numbers of records by primary Alert Reason

Primary Alert Reason	No. of records	Percentage	No. of records	Percentage
	(25 September 2006)		*(18 July 2008)*	
National security	72	11.6	97	12.6
War crimes or human rights abuses	7	1.1	7	0.9
Controversial visitors/weapons of mass destruction	2	0.3	2	0.3
Serious or high profile crime	15	2.4	19	2.5
Health concerns	11	1.8	9	1.2
Organised immigration malpractice	366	59.0	486	63.0
Child custody concerns	7	1.1	14	1.8
Other criminals	34	5.5	37	4.8
Overstayer	12	1.9	10	1.3
Breach of visa conditions	2	0.3	2	0.3
Debts to the Commonwealth	14	2.3	14	1.8
Immigration malpractice	38	6.1	51	6.6
Refused/bypassed immigration clearance	1	0.2	2	0.3
Suspect genuineness	36	5.8	16	2.1
Surrender Australian travel document	3	0.5	5	0.6
Travel sanctions	0	–	1	0.1
Illegal fishers	0	–	0	–
Serious criminal (poor bio data)	0	–	0	–
Total	**620**	**100**	**772**	100

Source: September 2006 data—DIAC analysis; July 2008 data—ANAO analysis of DIAC records. Australian citizens identified by being recorded by DIAC as such on the PAL record. Alert Reason indicated is the primary reason: some records also hold one or more secondary reasons.

Note: The ANAO's analysis identified some 243 aliases among the 772 records in July 2008. (The remainder comprise 117 'primary' records—those with one or more alias—and 412 records with no alias indicator.) This means that the number of actual persons identified by these records is probably 529, rather fewer than the number of records. However, the ANAO understands that before CMAL was implemented, DIAC MAL statistics generally refer to the number of records (including aliases) rather than the number of persons. Thus, for the purposes of making accurate comparisons, the number used in this table is the number of records.

4.22 There are several features worth noting in this analysis:

- First, the number of records has grown by nearly 25 per cent over the intervening 22 months.

- The distribution of records among Alert Reasons is similar in both analyses. Further, the proportion of records listed against *Organised Immigration Malpractice* is similar to that reported by the Wheen Review from data of June 2003.
- Only a few Alert Reasons recorded a reduction in numbers.

Other findings of the analysis

4.23 The analysis revealed other features in the data:

- *Most were overseas-born*. Of the records of Australians on PAL in July 2008, 12 per cent show Australia as the person's country of birth and 76 per cent have an identified 'other country' as their country of birth.[163]
- *Austrians and Australians are sometimes wrongly coded as each other*. Simple inspection shows some persons identified as Austrian citizens are, in fact, Australian citizens.[164] DIAC advises that 'unfortunately the main reason many are present [*is*] due to human error.'[165]
- *Most of the records are at least five years old*. Many of the records of Australians in PAL in July 2008 have been there for some years. The earliest was entered in 1996 and nearly one-third have been there since 2001. The total number has grown by 71 (ten per cent) in 2008 including 34 cases listed for organised immigration malpractice.[166]

Limited culling of organised immigration malpractice records

4.24 DIAC's internal review of progress with Wheen Review recommendations shows that, in July 2005, most of the 531 records of Australians on PAL at the time were *Organised Immigration Malpractice* cases and that a 'significant proportion may no longer be relevant'. Of the 486 *Organised Immigration Malpractice* records on PAL in July 2008, some 329 dated from 2004 or earlier. This suggests that there has been little culling action since, despite the specific

[163] A further four per cent had nothing recorded for their country of birth and, for the remaining eight per cent, it was 'unknown' (ANAO analysis).

[164] This was apparent either because the persons identified are well-known or the record was marked as an alias for another record which was identified as Australian.

[165] DIAC advice of 4 August 2008.

[166] Note that the ANAO analysis cannot reveal how many of the records present at any earlier time have been purged from the system. It can show, however, based on the creation date, how long records have been on the system.

decision in December 2003. During the audit, DIAC advised the ANAO that 'IAS is currently reviewing the list of Australians on PAL and liaising with the [CMAL] Data Management team and [*other officers*] to effect a clean-up.'[167]

4.25 Similarly, although there was a clear intention to remove Australians listed for certain other reasons in late 2006, the ANAO found 66 such cases still on PAL in July 2008, of which 57 dated from 2006 or earlier.

Narratives do not contain the required text

4.26 An inspection of the 71 records created in 2008—that is, since the relevant DIAC instruction was last updated (1 December 2007)—showed that in no case does the narrative contain the indication those instructions require that the citizen's cooperation be requested, and so on (see para. 4.18).

DIAC has taken some corrective action recently

4.27 When the ANAO drew DIAC's attention to the PAL records with 'Australian' in the citizenship field, the department reported action it had undertaken to review them. DIAC reported a range of interim results, including 64 deletions, 51 where the record was modified (for example, some were found to have been wrongly recorded as Australians). Most of the remainder were under review.[168]

4.28 In March 2009, DIAC provided further results of its data cleansing activity for Australians on MAL. This shows that, across PAL and DAL, DIAC found, in July 2008, a total of 1964 records of Australians, including 772 on PAL (consistent with the ANAO's analysis). A summary of cleansing action taken by DIAC since then shows that 835 records were deleted, 501 retained and 628 referred awaited data owner review, including all 507 referred to IAS. As of March 2009, DIAC's CMAL Operations Section believe that 635 records of Australians remain on PAL.[169]

4.29 There is also evidence that DIAC has been seeking the production of:

> a report on the Production MAL database that will compare the Australian passports file with the Person Alerts (PAL) file, and report on exact matches.

[167] DIAC, email advice of 17 September 2008.

[168] DIAC, email advice of 9 September 2008.

[169] DIAC advice of 19 March 2009.

> The CMAL Data Management team will then use this report to undertake further research, and remove MAL alerts where appropriate.[170]

4.30 The DIAC documents seeking this report on MAL note that there are a number of Australians who are the subject of MAL alerts and that 'some are justifiable cases.' This implies that others are not justifiable and shows that DIAC is aware of that fact. The papers also state that 'there have been recent instances of Australians getting unnecessarily referred [*to immigration officers*] at the border.'

DIAC could state more explicitly that Australians are on PAL

4.31 A publicly-accessible document, DIAC's annual return to the Privacy Commissioner, states, about MAL: 'the purpose of these records is to maintain a list of foreign nationals *and certain Australian citizens* whose entry may be of concern to the Australian Community' [emphasis added].[171] DIAC public documents about MAL—which may be accessed more often—do not refer to this fact (for example, the *MAL Fact Sheet* on DIAC's website).[172] There is a risk that this different treatment could be seen as unwillingness to be transparent.

4.32 The earlier discussion noted that DIAC has a rationale for listing some Australians on MAL. There is no obvious risk to DIAC if it were to mention explicitly in public information about MAL that it observes this practice. This is particularly so, given that it has said so in other public documents.

Conclusion—DIAC needs to review its handling of records of Australians on MAL

DIAC should clarify its policy

4.33 DIAC's policy on the inclusion of Australians on MAL is not currently coherent or complete. It has not fully clarified its reasons for wanting to list Australians on MAL nor, therefore, identified the specific characteristics that would justify considering Australians for listing on PAL. It would benefit from

[170] DIAC, TRIPS Health Check Project, Request to implement change into Production, Issue—Identifying Australian Passport Holders on MAL.

[171] See the *Register of Federal Personal Information Digests* on the website of the Privacy Commissioner: <http://www.privacy.gov.au/government/digest/index.html> [accessed 7 May 2009].

[172] See <http://www.immi.gov.au/media/fact-sheets/77mal.htm> [accessed 7 May 2009].

doing so and then confirming that there is a sound legal basis for each reason. It could then revise its PAM3 manual on this matter accordingly.

DIAC should complete its cull of unnecessary records

4.34 Although action has been recommended or begun several times to cull inappropriate records of Australian citizens, it has not been completed. Moreover, new such records are being entered.

4.35 The failure to cull records is attributed in DIAC's internal review of July 2005 to 'little priority being given to cleansing' PAL. A related question is the lack of clear responsibility for those records by various areas of DIAC—the question of data ownership. When policy has been clarified, its legal basis verified, and clear accountability has been set, DIAC will be in a position to more effectively cull inappropriate records of Australians on MAL.

Recommendation No.2

4.36 The ANAO recommends that DIAC:

- clarifies the circumstances in which it can properly record Australian citizens on MAL, consulting other agencies with an interest in MAL as appropriate;
- in this light, revises its policy and procedural guidelines for recording Australian citizens on MAL; and
- completes its review of records of Australians on MAL, and deletes records of Australians where they are inappropriately recorded.

DIAC response: *Agreed*

DIAC is commencing a review of this policy and the means to practically implement these policy settings for the listing of Australians, noting that there is a need to improve the mechanisms for reviewing MAL listings at significant milestone events for clients, in particular, applications for citizenship.

DIAC has an ongoing program of review of records of Australians on MAL. While the number of Australians recorded on MAL has increased since 1999, the actual numbers are very low, and have actually reduced significantly as a proportion of overall records.

Some Australian identities will continue to be listed in MAL as there are legitimate reasons to do so. The risks of listing this small group are low—DIAC has no power to prevent the departure or entry of Australian citizens so there can be no hindrance to their travel. The short term listing of carefully selected Australian passports, which have been reported lost or stolen, on the DAL, is an important measure to preserve the integrity of the Australian passport system and detect potential impostors.

5. Privacy and MAL

This chapter considers whether DIAC has appropriate assurance that its handling of personal data on MAL satisfies information privacy principles.

Privacy: what agencies are required to do

5.1 DIAC records personal information, including sensitive items, on MAL. Like other Commonwealth agencies, it must comply with the Information Privacy Principles (IPPs) set out in the *Privacy Act 1988*. The *Migration Act 1958* and the *Australian Citizenship Act 1997* also impose requirements for handling personal information. The ANAO considered whether DIAC had addressed privacy and compliance with the relevant legislation in relation to MAL.[173]

5.2 Generally, Australian government agencies must comply with eleven IPPs.[174] Some agencies, such as DIAC, have some similar requirements set out in their own principal legislation. The department's approach to privacy is set out in 'Safeguarding your personal information' (Form 993i).[175] This document explains DIAC's obligations under the three Acts mentioned above.[176]

5.3 DIAC's 2006 report *Identity and Risk*[177] shows that it has been attentive to the Privacy Act and is aware that this Act extends to non-citizens, whose details comprise most MAL records. The report notes that there are two key matters to highlight with respect to privacy legislation:

- The Privacy Act (Interpretation, Part II, Section 6) states that "personal information" means "information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." Therefore, all information about the identity claim, as well as the

[173] At the commencement of the audit, DIAC identified the Office of the Privacy Commissioner as a key stakeholder and client for CMAL Section (DIAC advice of 31 March 2008).

[174] These are based on the 1980 OECD guidelines governing the protection of privacy and transborder flows of personal data. See website of the Office of the Privacy Commissioner: <http://www.privacy.gov.au/government/index.html> [accessed 7 May 2009].

[175] See: <http://www.immi.gov.au/allforms/pdf/993i.pdf> [accessed 7 May 2009].

[176] The privacy requirements of these acts are discussed in the ANAO Audit Report No.24 2007–08, *DIAC's Management of the Introduction of Biometric Technologies*.

[177] DIAC 2006, *Identity and Risk*, Identity Branch, 9 May.

assessment of the identity claim, is deemed to be "personal information" subject to the terms and conditions of the Privacy Act.

- The Privacy Act (Part I, Section 5B) is explicitly extraterritorial, meaning that representatives of the Australian government must accord equal treatment to citizens and noncitizens with respect to the rights granted under the Act.

5.4 The ANAO considered:

- what action DIAC has taken to gain assurance that its administration of MAL meets privacy requirements; and
- DIAC's practice on the retention of MAL records.

What action DIAC has taken on privacy and MAL

Conducting a Privacy Impact Assessment is sound practice

5.5 The Privacy Commissioner provides guidelines for the conduct of a *Privacy Impact Assessment* (PIA), a process to identify and recommend options for managing, minimising or eradicating a project's privacy impacts.[178] They state:

> A PIA can assist agencies to manage privacy impacts by providing a thorough analysis of the effect of the project on individual privacy and helping to find potential solutions. In many cases, a PIA can help to make a significant difference to the privacy impact of the project whilst still achieving the project's goals. The elements that make up a PIA (including identification, analysis and management of privacy impacts) help agencies to drive good privacy practice and underpin good public policy in their projects.

5.6 Performing a PIA is an example of sound practice in handling personal information. The guidelines include a threshold step of considering whether a PIA is appropriate. This shows that if a project involves the collection, use or disclosure of personal information then 'some form of PIA will probably be necessary.'[179] The CMAL project self-evidently involves personal information including some that DIAC considers sensitive.

[178] See: <http://www.privacy.gov.au/publications/pia06/index.html#mozTocId591260> [accessed 7 May 2009].

[179] See: <http://www.privacy.gov.au/publications/pia06/mod-a.html> [accessed 7 May 2009].

5.7 According to the guidelines, generally, the agency undertaking the project will be responsible for deciding if a PIA is necessary or desirable and then ensuring it is carried out.

DIAC took steps to begin a Privacy Impact Assessment for CMAL

5.8 DIAC has not considered privacy aspects of MAL recently.[180] However, in November 2006, DIAC's CMAL Project Team sought to have a PIA done for CMAL. This was welcomed at that time by an officer in the department's Privacy area, who explained:

> a PIA involves business areas identifying what types of information flow through their processes or practices to see if that information falls within the definition of 'personal information' and then considering whether they collect, store, access, use and disclose personal information in conducting their day-to-day activities. To help conduct the assessments, the Privacy Section formulated the Privacy Impact Checklist which has a number of flowcharts as well as a detailed Checklist which I work through with the business area to identify how information travels through their processes and what mechanisms are in place to protect privacy.[181]

5.9 Nothing eventuated. DIAC's Privacy Section advised the ANAO that in the early days of DIAC's SfP computer systems redevelopment, it had advertised its ability to undertake PIAs: 'CMAL did not respond and there was no capacity to pursue them.'[182]

5.10 In fact, there was the initial response from the CMAL team mentioned above but no record of further work. The current CMAL project team 'has no memory' of the exchange on the PIA.[183] DIAC stated:

> although a Privacy Impact Assessment was listed as an item [*in earlier CMAL work*], it appears that it has not been pursued. A possible reason is that privacy is about information not processes (especially IT processes). As CMAL was not about changing the fundamentals of the information contained on MAL about an identity, whatever existing privacy issues will still be valid.[184]

[180] This is based on the recollections of current staff in DIAC's Privacy area, who advised that 'Privacy [*Section, DIAC*] has not been consulted about MAL in the past.' DIAC email advice of 12 May 2008.

[181] DIAC, email from Privacy Section to CMAL Project team, 6 November 2006.

[182] DIAC, email advice of 20 May 2008.

[183] DIAC, email advice of 23 May 2008.

[184] DIAC, email advice of 17 June 2008.

5.11 The argument here is that, since CMAL was not changing any practices in the use of personal data but redeveloping the IT processes to handle that data, then CMAL, of itself, would not have a privacy impact. DIAC has given a similar response more recently to a Senate Committee. Here, DIAC was asked if there had been a PIA for the new Border Security Portal.[185] DIAC responded:

> The development of [the] Border Security Portal does not introduce any new sources of client information nor does it alter any practices in relation to access and disclosure of client information. For this reason a Privacy Impact Assessment was not undertaken.[186]

5.12 However, since there has never been any systematic analysis of the privacy impact of MAL in the first place, arguments about new systems not changing practices are beside the point.

5.13 The legal advice DIAC had received in late 2002 about its practice of keeping records of Australian citizens on MAL was explicitly contingent upon it complying with, *inter ali*a, the Privacy Act (see para. 4.7). However, there has been no analysis of DIAC's compliance with IPPs even though DIAC's subsequent approach to recording Australians on MAL rested on this advice.

Certain related privacy work was specifically funded

5.14 In the 2005–06 Budget, the Government announced that:

> The Government will provide $0.7 million over four years for the Office of the Federal Privacy Commissioner (OFPC) to address privacy issues arising from the implementation of biometrics for border control.[187]

5.15 When the ANAO examined DIAC's management of the introduction of biometrics, it reviewed whether DIAC had developed a robust framework for administering privacy requirements. The ANAO concluded that DIAC needed to strengthen substantially its processes for assuring itself that it meets requirements for handling personal identifier and related information.[188]

[185] A project under SfP which provides staff with access to various Departmental systems, including CMAL.

[186] Budget Estimates hearing of 28–9 May 2008. See: <http://www.aph.gov.au/Senate/committee/legcon_ctte/estimates/bud_0809/diac/index.htm> [accessed 7 May 2009].

[187] DIAC, Portfolio Budget Statement 2005–06, p. 88.

[188] ANAO Audit Report No.24 2007–08, *DIAC's Management of the Introduction of Biometric Technologies*, pp. 83–8.

5.16 DIAC provided evidence that it had 'sought comments' in March 2007 on the CMAL project from the Privacy Commissioner. DIAC's Identity Branch had provided a briefing to the Privacy Commissioner's staff on CMAL and the Identity Services Repository. This is an underlying facility which supports both the department's biometrics developments and CMAL. Indeed, DIAC's biometrics project is a related area, managed within the same DIAC division. DIAC did not provide a record of the briefing it had given. There was clearly no substantial consideration of MAL in this process.

Retention of MAL records

5.17 DIAC provides details of its personal data holdings, and to whom it gives copies or access, to the Privacy Commissioner each year. The Privacy Commissioner publishes this information—the Personal Information Digest (PID).[189] The DIAC PID explains that '[MAL] records are kept for ... between 1 month to 120 years'. This suggests that MAL records are not kept beyond their expiry dates.

5.18 DIAC's PAM3 manual states that, in fact, all MAL records are archived when 'deleted'. Once archived, records cannot be reactivated or changed in any way. However, they may be viewed by officers with the right MAL access.[190] The implication is that DIAC keeps archived records indefinitely. The manual does not explain the reasons those officers might have for viewing such records.[191] The PID DIAC gives to the Privacy Commissioner does not mention the archiving procedure nor that such records can be viewed by certain officers.

5.19 The Migration Act (at s. 336K) provides an imperative to destroy identifying information as soon as possible after the *Archives Act 1983* no longer requires it to be retained. Also, s. 336L provides authority for DIAC to retain identifying information relating to non-citizens indefinitely in certain

[189] The information is published on the Privacy Commissioner's website. Each year Australian government agencies must maintain a record setting out the nature of the various types of records of personal information kept by the agency and related details in a Personal Information Digest. This submission is a requirement under IPP 5. See: <http://www.privacy.gov.au/government/digest/index.html> [accessed 7 May 2009].

[190] DIAC, PAM3, GenGuideA—MAL (Movement Alert List)—Policy and Procedures, p. 74.

[191] Even if it has been archived it is not clear that this excuses DIAC from the IPP requirement to keep the information up-to-date if those archived records can be viewed for some (unspecified) purpose. However, if archived records cannot be reactivated or changed in any way information in them may cease to be accurate and the officer viewing the record may be unaware of that.

circumstances.[192] Although each of these circumstances is likely to cause a MAL record to be created, the circumstances specified do not encompass all categories of PAL records: for example, criminals are not included. Therefore this section could not be relied on generally for retaining MAL records indefinitely.

5.20 A review of DIAC's 'records disposal authority' (RDA)—an arrangement under the *Archives Act 1983* with the National Archives of Australia—has been under way since 2003.[193] DIAC has advised that it had included disposal of identifying information in the review of the RDA.

5.21 In February 2009, DIAC advised that:

> DIAC accept that we will need to review and express the circumstances under which we are able to maintain data on potential clients of interest. We will need to ensure that our policy and procedures reflect what the various items of legislation do and do not allow us to do. We accept that we will need to express a clear distinction between client data and potential client of interest data, biometric and bio data and how long we are obliged or able to retain data in each category. DIAC have agreed that a privacy impact statement is required for MAL and plans to initiate the activity to complete this.[194]

Conclusion—management of MAL would benefit from a Privacy Impact Assessment

5.22 DIAC is aware of the importance of privacy of personal information and the relevant requirements of its own legislation and the Privacy Act. It is also aware that MAL very largely comprises personal information, some of which is sensitive. DIAC has not considered the privacy implications of its use of MAL in any substantial way. At one point, the department contemplated but did not proceed with a PIA for MAL during its CMAL project. It is apparent from the foregoing analysis that DIAC would be better able to assure itself that it satisfies the IPPs if it were now to conduct a PIA of its administration of MAL. The department has agreed to do so.

[192] These include where the non-citizen is or has been in detention, has been refused a visa or had one cancelled, becomes an unlawful non-citizen, has been removed from Australia or where the minister is personally satisfied the person is a threat to Commonwealth, State or Territory security and, in the public interest, issues a conclusive certificate to that effect.

[193] ANAO Audit Report No.24 2007–08, *DIAC's Management of the Introduction of Biometric Technologies,* p. 86.

[194] DIAC advice of 16 February 2009. DIAC did not state a timeframe for conducting the PIA.

6. MAL data-matching

This chapter considers how DIAC has managed arrangements for performing matches with its MAL records.

Data-matching fundamentals

6.1 A MAL-check involves comparing the data supplied by the visa or citizenship applicant or person seeking to enter Australia at the border against the data stored on MAL. This is the data-matching process. DIAC checks each person and their travel document against MAL on several occasions. These include when the visa application is lodged, when the applicant is at the overseas check-in (DAL only), while the flight is *en route* to Australia and when the applicant crosses the border and enters the country (see para. 1.6).

6.2 In 2007–08, about 6.1 million foreign nationals reportedly entered Australia.[195] Because of the numbers of travellers, it is impracticable for DIAC to check MAL manually each time. Therefore, checking has two stages:

- first, a computerised check uses software that searches and matches the input record against records on MAL. The system calculates a 'score' for each match and then, by discarding those below a specified threshold score, generates a short-list of results—potential matches or 'MAL notifications'—that require human judgement to resolve whether they are true matches.

- second, the human check then completes the process. A DIAC officer either confirms the case as a 'true match'; or discounts it.

6.3 Therefore, DIAC needs to use computer software skilfully, which includes 'tuning' it, to pre-sort potential matches so it can tell how good a match each case is. Then it needs to set a threshold score at a level that ensures that all of those worth checking go to human operators for consideration. These two stages and concept of the threshold score are explained in more detail below.

[195] DIAC, *Immigration Update 2007–08*, Section 3, Overseas arrivals and departures, Table 3.1, Summary of total movement, 2003–04 to 2007–08, p. 30, <http://www.immi.gov.au/media/publications/statistics/> [accessed 7 May 2009].

Stage one: the preliminary computerised check

In the computerised check, for each case, the software calculates a match score out of a maximum of 100. The higher the score, the greater the likelihood of a true match and that the person is the same as listed on MAL.

The software calculates this score using rules DIAC develops. DIAC adjusts these rules by testing the results the software generates against those expected from human judgement using subject matter experts. This lets DIAC 'tune' the software to optimise matching performance, having regard to the circumstances (combinations of names, typical errors and so on).

Even after 'tuning' the software, the rating score is only a general guide to the likelihood of a match being a true match. A true match can attract a relatively low ranking score. Therefore, human consideration is vital to distinguish true matches. The software completes its assessment by presenting only those results with a match score greater than a predetermined threshold.

Stage two: human match resolution

MAL match cases are presented to DIAC's BOC staff for the second stage of matching. During the audit, the system was presenting cases for resolution at an average rate of about 4000 within each 24-hour period. This can vary from 500 to 10 000.[196] Each match case contains one or more potential matches—with an average at the end of the audit period of 12 per case. True matches are relatively infrequent: DIAC advises that just over 1 in 200 matches yields a true match, resulting in around 5.5 per cent of match cases being resolved as a positive match.[197]

Once a match notification is presented to a BOC officer, they consider it and resolve it. They examine each notification on screen, considering side-by-side both the applicant's data and the relevant MAL record, which the preliminary check has identified as a potential match. If the BOC officer decides the identities are the same this is found to be a true match. Otherwise, it is a false match and needs no further consideration. Once all potential matches are resolved for a particular applicant, an informed decision on the visa/citizenship application or entry to Australia can be made.

[196] DIAC, CMAL Project Implementation Plan, SfP8, p. 4.

[197] DIAC advice of 22 January 2008.

If the rules in the software are set optimally, true matches will correlate well with high match scores. ***However, it is impossible to write rules that will do this perfectly.*** This is because of the variability and complexity of naming practices, potential for errors and so on in the real world. From time to time, matches that turn out to be true matches attract only a relatively low score. Therefore DIAC officers must carefully consider all potential matches presented by the preliminary check.

Setting the threshold score

Setting the threshold score determines which potential matches the computer presents for human consideration. Any match below the threshold is not considered further. DIAC must set a score which provides assurance that, with a high probability, true matches will attract a higher score and will be presented as potential match cases. DIAC can never be certain that all true matches will generate a score above the threshold and the approach presents an ineradicable risk, albeit small. DIAC can control this risk and reduce it to a practical minimum by 'tuning' its software effectively.

In deciding the threshold score, DIAC is balancing two risks:

- If it is set high, it will find fewer potential matches but will increase the risk of missing a true match.
- If it is set low, it must devote more resources to resolve potential matches, but it has less chance of missing a true match.

A low threshold is associated with a risk-averse but resource-intensive approach. However, the number of matches requiring human consideration rises very rapidly as the threshold is lowered, and the frequency of true matches to be discovered at lower scores is much lower. A lower threshold also increases the risk of vigilance-fatigue among staff considering match notifications, and this, in turn, increases the risk of a true match being missed.

6.4 In considering DIAC's data-matching practices, the ANAO examined:

(1) *DIAC's development of MAL data-matching.* In particular, the ANAO examined what DIAC had learned to help improve its data-matching over the last decade, including as a result of the various MAL reviews.

(2) *Whether DIAC has adequate data-matching tools to perform MAL-checks.* This includes adequately tuned data-matching software and an appropriate threshold score in place, enabling DIAC officers to avoid unnecessary risk to make the best informed decision.

(3) *Whether DIAC seeks continuous improvement of its data-matching practices*. This includes analysing performance reports and fostering a continuous improvement culture.

(1) DIAC's development of MAL data-matching

6.5 During the 1980s, DIAC used Name Search Software, (NSS) for its preliminary MAL-check. It developed NSS in-house and implemented it across all visa-processing systems worldwide. Since then, the major reviews of MAL have addressed the (i) selection of matching software and (ii) setting the threshold. This section discusses development of data-matching over the past decade in the light of these reviews.

Better data-matching software

6.6 In 1997, DIAC failed to detect the entry of a known criminal, Lorenzo Ervin, who was listed on MAL. This led to the Sadleir Review in 1997–98, which included an examination of MAL and its data-matching practices. Before the Sadleir Review was complete, DIAC began to implement more sophisticated name-search software called 'SSAName3' (version 1.7). This is more capable than NSS of recognising possible matches where names have been transposed or mis-transcribed, or data is sparse, and so on.

6.7 DIAC's principal visa processing systems are:

- IRIS, which operates 'offshore' (that is, at its overseas posts);
- ICSE, which it uses in Australia for visa and citizenship processing; and
- ETAS, its ETA system, operated by a contractor, and which works through the travel industry network and Internet.

6.8 In every case DIAC subsequently enters records of all visas issued using these visa processing systems into its TRIPS system in a process called 'visaload'. DIAC decided to implement the new matching software at the visaload process (and, later, ICSE) but not in the offshore system, IRIS, or ETAS. In effect, the secondary check at visaload provided a backup-check for each visa granted in all systems including IRIS and ETAS, creating a 'tiered' approach to MAL checking, endorsed by the then minister. A later review explained:

> one of the considerations for not implementing the name search software [in IRIS] was the cost of procuring the licenses. Another factor was using the

software in a non-mainframe environment and possible demands on overseas IT infrastructure.[198]

6.9 Conducting a thorough check at visaload process only has its risks:[199]

- if a match were detected at visaload that had been missed in the off-shore check, the visa would already have been issued and the visa-holder may have been in transit. There might have been only a short time for DIAC to act before the visa-holder sought to enter Australia;
- it is easier for DIAC to refuse a visa then to cancel a granted visa;[200] and
- the process provided an incentive for staff at posts to rely on the backup rather than check matches thoroughly, or even to check at all.

6.10 This last risk was later recognised in a letter to all posts from the then DIAC Secretary, in 2005:

> Staff should not rely on the secondary check to pick up on any matches missed at the application processing stage as there is a significant danger that matches that are not identified until the visa has been issued will result in travel by the individual to Australia. This represents a risk to national security.[201]

6.11 After the first implementation of SSAName3 in 1997, later reviews continued to recommend its extension to all of DIAC's processing systems. The Gerlach Review (2000) recommended that DIAC ensure: 'alternatives to the use of NSS are fully explored.[202] DIAC's Internal Audit Report in 2003 recommended that DIAC continue to investigate implementing SSAName3 in IRIS and ETAS,[203] which DIAC agreed to do.[204]

6.12 Finally, the Wheen Review discussed future priorities for MAL, stating: 'as the entries on MAL change, the name matching software must be re-evaluated and re-tuned. This needs to be part of an overall strategy to keep

[198] DIAC, Internal Audit of MAL, 2003, p. 12.

[199] Note that this describes the pre-CMAL arrangement.

[200] DIAC, Good Decision Making, Training for DIAC decision makers, v1.08 p. 51, April 2008.

[201] DIAC, letter from Secretary, March 2005.

[202] DIAC, Gerlach Review, Recommendation 23, p. 11.

[203] DIAC Internal Audit 'Review of the Movement Alert List in a Business and System context, 2003.

[204] DIAC advised (22 January 2009) that adoption of SSAName3 was considered by the IRIS area but the IRIS business owner assessed the cost of acquiring a licence, which was outweighed by the fact that CMAL was to be delivered shortly and it would effectively provide SSAName3 to IRIS without the need of a separate licence or additional development activity.

MAL operating at optimal effectiveness.' The review recommended that DIAC investigate the creation of a centralised MAL system, and upgrading its data-matching software.[205]

6.13 Implementation of CMAL in all DIAC's visa processing systems in late 2008 means that all MAL checks are now performed using DIAC's best available matching software on every occasion.

Controlling the setting of the threshold score

6.14 After the Lorenzo Ervin incident in 1997, the then minister had directed that the threshold determining cases for human consideration be reduced.[206] The Sadleir Review later commented:

> It is important the person bearing responsibility for setting the threshold should, in making a decision, have a lucid understanding of the wide implications and possible consequences of each of the broad options available. As a matter of routine, the officer responsible should seek guidance from the Secretary of the Department and, as necessary, the Minister. Thus, it is essential the officer responsible is at Senior Executive level.[207]

6.15 The Gerlach Review noted in 2000 that the minister was involved in setting the threshold score for visaload checking. However, DIAC alone set the threshold for offshore systems. This review recommended all threshold scores require executive/ministerial approval.[208]

6.16 In contrast with DIAC's Canberra-based systems, posts used to be able to adjust their threshold in their local copy of IRIS. They could do this without the knowledge of DIAC National Office. Until 2004, DIAC National Office has not always known what the threshold scores have been at any given time and, at times, has found it challenging to impose requirements on its posts.

6.17 DIAC had attempted a stock-take of all individual post's threshold scores in 1997, in preparation for the Sydney Olympics. This found the Wellington post had adjusted its score to 94, the highest of any post. This reduced the number of potential match notification sent for resolution and

[205] Wheen Review, p. 8.

[206] DIAC evidence to a Senate Estimates hearing, Hansard, 21 August 1997, p. 71.

[207] Sadleir Review, p. 19.

[208] Gerlach Review, 2000, Recommendation 7, p. 9.

increased the risk of a true match being missed. Auckland was among a small number of posts who did not report their score at this time.[209]

6.18 In March 2003, a MAL match for a potential *National Security* case with a score of 93 was *not* presented to the Auckland post, as its threshold was 94. An internal DIAC investigation followed and the post confirmed the setting.[210] National Office replied: 'given our recent experience, I would appreciate it if you could please consider dropping this to at least 90 for the time being.'[211]

6.19 In June 2003, when the question of posts' threshold scores came to attention, a senior officer in the MAL area in DIAC's National Office commented:

> [I] haven't a clue what [*threshold score*] settings individual posts have decided on and what criteria they used to decide. And they can change again tomorrow without us being aware.[212]

6.20 DIAC commenced another extensive investigation to the threshold scores individual posts had set, concluding in April 2004:

> Posts have varied local settings to adjust to local conditions. However, any future changes should not be made without prior approval from the Assistant Secretary, Entry Policy and Systems Branch.[213]

6.21 Subsequently, DIAC National Office monitored all post threshold scores by incorporating a 'threshold score' column into management reports. A post setting its threshold higher than 85 would create a warning. DIAC advises that, after this measure, no post set its threshold above 85.[214] Since Sadleir had warned of the critical nature of threshold setting in 1998 and this was repeated by the Gerlach Review in 2000 it is not clear why it took another four or five years to impose department-wide discipline.

6.22 Again, implementation of CMAL addresses this matter completely by having all data-matching being performed on the one copy of MAL, with thresholds under the control of DIAC's National Office. DIAC advises that all

[209] DIAC minute, 30 October 1997.

[210] DIAC minute, 11 March 2003.

[211] DIAC, email 16 May 2003.

[212] DIAC, email 5 June 2003.

[213] DIAC, email 6 April 2004.

[214] DIAC email to ANAO, 26 June 2008.

risk levels now have the same match score threshold. However, DIAC also advises that variable match threshold scoring is currently under design for CMAL, as operational experience now suggests that a variable threshold will deliver substantial workload savings with no or minimal increased risk of missing needed matches.[215]

(2) DIAC has the correct tools to perform MAL-checks

6.23 Following government endorsement of the recommendations of the Wheen Review in 2005, DIAC began investigating enhanced data-matching tools. This review had made several recommendations relevant to DIAC's upgrading its data-matching practices. Consequently, DIAC undertook:

- preliminary investigations on its then current data-matching situation including assessing the version of the software.[216] In the light of the results, DIAC began work on upgrading; and
- a comparison of the merits of mainframe versus mid-range server processing for name searching.[217] It completed this in April 2006.[218]

Appropriate consideration was given when choosing the software

6.24 DIAC's Border Systems Board considered four options along with projected impacts, benefits, timeframes and budgets and, in February 2006, agreed to upgrade the software to version 2.6. DIAC began the MAL Augmentation Search Capability (MASC) project to implement the software upgrade. Its objectives were, *inter alia*, to improve on the then current search capability and to implement a version of SSAName which would be more easily and efficiently maintained by the business and technical areas.[219]

[215] DIAC advice of 22 January 2009. A similar arrangement has existed earlier: in July 2000, the then minister approved threshold scores of: 74 for High, 78 for Medium and 82 for Low Risk alerts (Wheen Review, p. 66).

[216] DIAC, internal minute Upgrade of Name Searching and Matching software in MAL, circa end 2005.

[217] Wheen Review, Recommendation 8.29 p. 48.

[218] DIAC, Name Search Research Infrastructure, 26 April 2006.

[219] DIAC, MASC Project Management Plan v0.5 p. 8.

6.25 Senior DIAC officers approved the MASC project closure report in February 2007.[220] This asserted that the project met its stated outcomes and objectives.[221]

The matching software underwent thorough testing and tuning

6.26 As the number of MAL records and potential notifications increases, the data-matching software requires further tuning to optimise its performance. The Wheen Review proposed DIAC give a high priority to examination of the settings and tuning of the name searching systems so as to produce fewer but better quality potential matches.[222] The MASC project conducted the first tuning process of the MAL data-matching software in six years. A DIAC paper on the name-search functionality states:

> It was revealed that the algorithm [*that drives the data-matching for the MAL database*] hadn't been tuned … for over six years [*as at 2006*] … during that time the disaster [*of 11 September 2001]* had struck, changing the focus of MAL to one of national security over simpler border protection issues.[223]

6.27 The rules that the software follows when identifying potential match notifications are determined when tuning the database. Each tuning is specific for the outcomes required with the then current database. It involves testing the data for expected results and calibrating rules the software uses based on the results of a series of tests.

6.28 DIAC provided evidence it had thoroughly tuned and tested the software using the following techniques:

- The project team tested the performance of the tuned software using a copy of the complete MAL database. It tested the software's handling of cases which had been problematic with the previous, untuned version of the software. This ensured that known problems were tested and accounted for.
- Subject matter experts conducted the tests, comparing the results of the software against a series of known expectations. If the software did not produce the expected results then additional tuning was required.

[220] DIAC, SSAName Upgrade MASC001 IT Project Closure report, February 2007.

[221] In fact, a software module was not correctly implemented. See Chapter 8.

[222] Wheen Review, p. 8.

[223] DIAC, Systems for People, Client-Centric project (SFP006) November 2007, p. 7.

> Some expected results could include dealing with the transposition of names, discounting double-letters and vowels, and so on.

6.29 Rather than building an entire testing platform, DIAC used an existing platform held by another Commonwealth agency which had previously upgraded similar data-matching software.

(3) DIAC seeks further improvement of its data-matching

DIAC plans to tune its data-matching tools regularly

6.30 Because MAL continues to grow and change, the imperative remains for DIAC to undertake further tuning for optimum data-matching outcomes.

6.31 DIAC has recognised the imperative for regular tuning. It has proposed to establish a permanent unit—the 'Business-As-Usual' (BAU) unit—within DIAC. The BAU would maintain the work of the MASC project, continuously tuning and monitoring the software. This capacity is desirable given the volume of new records being entered on to MAL.

6.32 The BAU proposal document of November 2007 states:

> Since the [*SSAName3 version*] 2.6 algorithm went live in November 2006, there has been a 50% increase in the records loaded within MAL. With that rate of change, by the same time next year (2008)… such a circumstance would make the MASC [*project*] tuning [*exercise*] far less efficient (or even relevant) than it was when implemented.[224]

6.33 In January 2007, the recommendation to establish the BAU was presented to the DIAC Systems Committee. DIAC advises that BAU support for the Name Matching team had been provided within the Border Operations Branch since January 2007.

DIAC seeks to widen its data-matching ability

6.34 Other Commonwealth agencies with a role for identity matching have previously commented on the vulnerabilities that arise from relying on name-based identity checks which do not have the capacity to incorporate a link to other identifying information, including biometric identifiers.[225]

[224] DIAC, Systems for People, Client-Centric project (SfP006), p. 7

[225] 'Biometric' is information drawn from a person's characteristics that is relatively unique and unchanging.

6.35 A system which links to a biometric identifier reduces certain risks that arise with name-based searches. For example, it is easy and lawful for a person to change part, or all of their name. People can do this repeatedly. This potentially allows people to create numerous identities which are difficult to link. A unique biometric identifier linked to a name-based record minimises the risk of not detecting a person who poses a threat to the Australian community.

6.36 Therefore, it is likely that future practices of data-matching will include biometric factors. This could include fingerprint, facial or iris recognition, amongst many options.

6.37 The minute to the minister setting out terms of reference for the Wheen Review stated (in September 2003):

> In planning a new generation of MAL we will be seeking to enhance its capacity to identify people of interest by enabling it to access identification technologies such as facial recognition and fingerprints and to have a profiling capacity beyond what it currently has.[226]

6.38 Consistent with this, the Wheen Review recommended that DIAC investigate such methods for future identity matching on CMAL, including:

> The architecture of NEWMAL [*CMAL*] be designed to enable MAL to take advantage of biometric technologies as they are proven for MAL's purposes.
>
> and
>
> NEWMAL [*CMAL*] should have the capacity to include images, if pilot testing demonstrates the practicality of such a facility.[227]

6.39 DIAC has undertaken research on future identity matching methods. The current DIAC strategic plan for identity management states:

> Supporting biometric capabilities and tools are still being developed and progressively deployed – there still remains much to do before a mature and fully integrated identity management capability is delivered.[228]

6.40 It is notable that neither MAL nor CMAL are specifically mentioned in DIAC's strategic plans on identity management. Therefore, it is not clear that

[226] DIAC, minute from the Executive Co-ordinator, Border Control and Compliance Division, to the Minister for Immigration and Multicultural and Indigenous Affairs, 17 September 2003.

[227] Wheen Review, 2004. s 21.8 and s 21.9 p. 99.

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

DIAC's initial work on biometrics has, so far, followed through on its imperative to relate new biometric technologies and MAL.

6.41 The ANAO's audit of *DIAC's Management of the Introduction of Biometric Technologies* in 2007 recognised the difficulties of implementing a biometric platform in a rapidly changing technological environment. It recommended that DIAC assess broadening its capability to include such available data as facial images and fingerprints for watch-lists and other identification purposes. DIAC agreed.[229]

6.42 DIAC advised that its future strategy, linking MAL and biometrics is now as follows:

> As part of DIAC's *Identity Management Strategic Plan 2007–10* (Identity Matters), the Department is establishing an identity services capability. The purpose of identity services is to manage the complex relationship between personal information, credentials and biometric data. The capability comprises a suite of enabling tools that includes the data repository as well as software and processing engines to manage the biographic information, documentary details, digital facial images and other biometric data.
>
> A biometric watchlist for facial images and finger scans forms part of this capability. The watchlist for facial images will be deployed as part of Systems for People releases in March and June 2009. Initially, the facial image watchlist will comprise images of missing persons provided by law enforcement agencies. The finger scan watchlist will become operational when DIAC is able to match against the National Automated Fingerprint Identification System managed by CrimTrac (including Interpol Red Notices). This is expected to occur by end 2009.
>
> Once these biometric watchlists are operational, they will form complementary alert systems covering both biographic (MAL) and biometric elements. Further development of these systems in the medium term could, for example, include the provision of facial images by law enforcement or security agencies for entities on MAL for inclusion in the biometric watchlist. Development of the systems will be iterative. As with the tuning of name matching software, it is important to ensure the biometric matching engines are providing accurate matching results before the watchlist galleries are expanded significantly.[230]

[229] ANAO Report No.24 2007–08, *DIAC's Management of the Introduction of Biometric Technologies*, p. 23.

[230] DIAC advice of 19 March 2009.

Conclusion—future strategy links MAL and biometrics

6.43 Over the last decade DIAC has gradually extended sophisticated data-matching software to its visa processing and border operations systems. CMAL has enabled DIAC to address the main risks the department was formerly exposed to of not using its best data-matching software in each visa processing system and varying threshold scores. DIAC has recognised the need to continually tune and refine this software.

6.44 DIAC now has a strategy encompassing biographic (MAL) and biometric elements, acknowledging that identity management will become a more complex task in future.

7. MAL's interaction with migration law

This chapter considers how DIAC's use of MAL interacts with migration law.

MAL: the interaction of administrative and legal authority

7.1 MAL processing is an administrative activity: it is not mentioned or referred to in migration or citizenship law.[231] While DIAC's use of MAL is based wholly on administrative authority, it has become an essential tool in applying migration law in particular.

7.2 To examine the relationship between legal and administrative authority in DIAC's use of MAL, the ANAO addressed the following questions:

(1) whether migration law places any constraints or requirements on DIAC's use of MAL in granting visas;[232]

(2) whether DIAC can direct its delegates in their use of MAL; and

(3) whether DIAC delegates must await the outcome of a MAL check.

(1) Constraints or requirements on DIAC's use of MAL

7.3 The Migration Act sets out exhaustively how visa applications must be dealt with. That is, it states all the things that need to be done to decide visa applications.[233] The object of providing an exhaustive statement of procedure is to replace the common law 'hearing rule.' However, in achieving this objective it excludes as unnecessary any actions other than those it provides for in deciding visa applications: there is nothing else a delegate must do beyond those things set out in this part of the Act.

7.4 The joint Administrative Review Council–DIAC guide *Decision-Making: Natural Justice* notes that: 'the courts have interpreted the exhaustive codes of

[231] DIAC, response to the ANAO's 'Preliminary questions for the Department of Immigration and Citizenship' before the performance audit commenced, 31 March 2008.

[232] The ANAO also examined the basis on which DIAC officers consult MAL in making decisions on applications for Australian citizenship. It found that there is nothing in the Australian Citizenship Act or the Australian Citi¬zenship Instructions (ACIs) that requires officers to consult MAL. However, in practice, the ICSE computer system they use requires a MAL check to be made as a part of normal citizenship processing.

[233] See Part 2 of the Act, Subdivision AB (ss. 51A–64).The 'Code of procedure for dealing fairly, efficiently and quickly with visa applications' declares (at s. 51A (1)) that it provides an exhaustive statement of the natural justice hearing rule in relation to the matters it deals with.

procedure in the Migration Act to be complete procedural codes as a result of the introduction of s. 51A of this Act' (p.9). This state of affairs is also reflected in DIAC's PAM3 manual:

> The codes [of procedure] exhaustively set out the procedural steps that decision-makers, including the Tribunals, are required to follow to deal "fairly, efficiently and quickly with visa applications."

Part of the code provides for MAL to be consulted

7.5 Section 56 (1) of the Migration Act reads:

> 56. (1) In considering an application for a visa, the Minister may, if he or she wants to, get any information that he or she considers relevant but, if the Minister gets such information, the Minister must have regard to that information in making the decision whether to grant or refuse the visa.

7.6 DIAC confirmed that this section allows the minister to get information from any source and that this is the section that allows the use of MAL for visa decision-making.[234]

7.7 A consequence of this view is that, if the delegate gets information under that section, he or she must have regard to that information in making the decision to grant or refuse the visa. In the case of MAL that would mean, if a delegate considering an application gets information from MAL, they must have regard to that information in making their decision. This, in turn, means that some reference to that information (though not necessarily the fact that MAL drew attention to it) must be discernible in the decision record, especially where the information provided by MAL provides a reason for the decision.

(2) Whether DIAC can direct its delegates in using MAL

7.8 DIAC advised the ANAO that 'it is a policy requirement for all visa processing that the decision-maker check whether a visa applicant has a MAL record and take that information into account when making the visa decision.'[235] DIAC instructions place an obligation on visa processing officers to

[234] DIAC, undated advice, Legal Opinions Section, circa 13 May 2008. The Explanatory Memorandum for the amending Act that introduced this section reads, in relation to s. 56: 'This section expressly allows the Minister orally or in writing to seek any further information the Minister considers relevant, *from any source*, including the applicant [*Emphasis added*]'.

[235] DIAC, response to the ANAO's 'Preliminary questions for the Department of Immigration and Citizenship' before the performance audit commenced, 31 March 2008.

consult MAL before making a decision on every occasion they consider an application. For example, DIAC's PAM3 manual, in the section on MAL, states that 'DIAC officers *must* check every application against MAL' [*emphasis added*].

7.9 On the other hand, s. 56 of the Migration Act places discretion squarely in the hands of the delegate as to whether they get 'any information that he or she considers relevant'. The minister—which includes delegates of the minister—may get this information *if he or she wants to*. They could elect not to get such information, if they should feel no need in a particular instance. If this is the avenue to obtain information from MAL then the section gives the delegate discretion as to whether they should do so. Policy cannot bind a decision-maker's discretion under the law.[236]

Minister can make directions but none has been made

7.10 Ordinarily, delegates must exercise their own discretion in making the decisions they are empowered to make. Their exercise of a delegated power cannot generally be subject to direction or conditions imposed by the person who delegates the power. This may be constrained where the law provides that the delegate is subject to directions or conditions imposed by the person who delegates the power. In that case, the person can issue non-binding guidelines to which a delegate is to have regard in the exercise of a power. Such guidelines cannot, however, require a decision-maker not to exercise his or her discretion.[237]

7.11 A provision for delegates of the minister to be subject to ministerial directions exists at s. 496(1A) of the Act and a provision for the minister to give directions to a person having functions or powers under the Act exists at s. 499. Directions could be given by the minister as to the process to be undertaken in making delegated visa decisions, including in relation to the power to seek information under s. 56.

[236] DIAC, *Good Decision Making: Training for DIAC Decision Makers*, version 1.08, April 2008, pp. 28–9.

[237] This argument is based on the general advice provided in AGS Legal Briefing No.74, Delegations, authorisations and the *Carltona* principle, 14 December 2004. See: <http://www.ags.gov.au/publications/agspubs/legalpubs/legalbriefings/br74.htm> [accessed 7 May 2009].

7.12 Ministerial directions under s. 499 are legislative instruments, recorded on the Federal Register of Legislative Instruments. No current direction states how a delegate is to exercise a power to seek information under s. 56.[238]

The risk of delegates not consulting MAL is probably low

7.13 As a matter of general practice, DIAC delegates do and will continue to consult MAL before making a decision. Indeed, as matter of practicality:

- DIAC visa processing systems do not allow the delegate to proceed to the point where they can make a visa grant decision unless MAL has been checked; and
- delegates have a substantive duty under s. 65 to satisfy themselves as to whether or not the criteria for the grant of the visa are met. Performing a MAL check is a primary means by which a delegate can test an applicant's claims against public interest criteria.

7.14 Delegates may regard making a MAL check as good practice. However, given that s. 56 is the legal avenue by which a delegate gets MAL information then they need only do that where they elect to do so. There is no provision for them to be instructed or compelled to do so.

(3) Awaiting the outcome of a MAL check

7.15 When a delegate undertakes a MAL check while considering a visa application it may take time for advice to be returned on whether there is a true MAL match. The ANAO considered whether the delegate could be instructed to await the outcome of the MAL check before making a decision to grant or refuse a visa.

7.16 The ANAO found that DIAC had considered this matter in 2007 at the initiative of the CMAL team.[239] To appreciate the relevant deliberations it is necessary to comprehend certain aspects of how CMAL works.

Decision-making under CMAL: the operation of the 'decision gate'

7.17 Under CMAL, when an applicant seeks a decision (such as a visa grant/ refusal decision) a feature of the decision-making process is a MAL 'decision

[238] Legislative Instruments can be viewed here: <http://www.comlaw.gov.au/> [accessed 7 May 2009].

[239] DIAC, minute of 15 January 2007 to the Director, Central MAL Project.

gate' in the computer system. This gate may be open or closed according to the status of the MAL check in respect of a particular case. Where the gate is open, a decision can be made without further ado. Where it is closed, DIAC expects certain actions to be carried out by the delegate before a decision is made. DIAC allows a closed gate to be overridden according to a set of rules and procedures it has devised. Under the arrangements proposed by DIAC, an authorised officer in the BOC would have had direct control of the gate and performed the override where it was required.

DIAC's internal consideration of the rules

7.18 DIAC's internal consideration specifically addressed the following questions: (i) to what extent direction could be provided to a decision-maker NOT to exercise an override and proceed to grant a visa where a possible MAL match had been identified and (ii) whether direction could be given as to when the override could be exercised or whether administratively restricting access to the override was permissible.

7.19 DIAC concluded that a visa decision does not turn on the criteria for the grant of the visa to be met; rather, that the delegate is *satisfied* that those criteria have been met:

> As it is the delegate's 'satisfaction' that the criteria for the grant of the visa have been met that is critical, it is neither lawful nor appropriate for a delegate to be directed not to grant a visa. In the event that such a direction was made, it is likely to be viewed by a court as having fettered the delegate's discretion and the decision to refuse to grant the visa as having been affected by a jurisdictional error.[240]

7.20 In considering whether a delegate can be directed to await receipt of further information from a MAL check before making a decision as to whether or not the applicant meets the criteria for visa grant DIAC concluded (in summary):

- if the delegate is genuinely satisfied that the applicant meets the criteria for grant of the visa to which the information on MAL relates, the visa

[240] DIAC, op. cit.

must be granted. Conversely, if the delegate is genuinely satisfied that the applicant does not, the application must be refused;[241]

- if, however, the delegate is undecided as to whether they are satisfied that the applicant meets the criteria for grant of the visa to which the information on MAL relates, *it would be open to the delegate to delay their decision* on the visa application until the receipt of further information.

7.21 An important point here is that the discretion to wait lies with the decision-maker, not any other officer, including any more senior one.

7.22 In considering whether access to the override could be restricted, DIAC concluded that it is the delegate who holds the decision-making power and the delegate alone who must ultimately make a decision without being subject to dictation. This means that:

- Managers or other officers can only give advice to delegates;
- Managers or other officers cannot direct delegates to make a certain decision;
- Delegates are not obliged to follow advice from managers or other officers in regard to whether an applicant meets a criterion for the grant of a visa, rather after giving due consideration to the advice given, delegates must reach their own decision;
- Where a manager or other officer 'directs' or places undue pressure on a delegate to decide a visa application in a certain manner, the delegate should escalate the matter.[242]

7.23 This view makes clear where the visa decision-making power lies: with the delegate and none other. The scheme of restricted access to the override then proposed by DIAC was thought unproblematic provided the 'authorised officer' who could trigger an override:

> is simply discussing with the delegate whether the applicant meets the criteria for grant of the visa to which the information on MAL relates, and then admin-

[241] This is based on internal legal advice provided to the CMAL project in January 2007. DIAC has later advised (22 January 2009) that there are cases where a delegate has the discretion to form the view that a public interest criterion has *not* been met but still to grant a visa. However, in the current argument this is a technical detail and does not detract from the thrust.

[242] DIAC, ibid.

> istratively recording, or authorising the recording of, the *delegate's* decision that the applicant meets, or fails to meet as the case may be, that criterion.[243]

7.24 This means that, if the practice proposed by DIAC meant that it would be the authorised officer that would be making the visa decision rather than the delegate, then that would be 'neither lawful nor appropriate'. It should be made 'extremely clear' to the officers authorised to trigger the override that in cases where they do not agree with the decision reached by the delegate, the former could not refuse the override.

DIAC's procedures may restrict the decision-maker's discretion

7.25 DIAC subsequently developed procedures for officers staffing the BOC relating to 'Override MAL Status'.[244] It is apparent that these have been drafted in the light of the internal consideration referred to above. However, it is not clear that these instructions have successfully negotiated a path between leaving the delegate's decision unfettered and ensuring that due care is exercised in visa decision-making by checking MAL first. For example, the procedures include statements such as the following:

> If the match case contains likely matches that need to be referred you should advise the DIAC Decision Maker that the case requires assessment by an Alert Owner before it can be finalised (p. 5).

7.26 The words 'requires assessment' leave no other options. Prima facie, this could reasonably be viewed as restricting the decision-maker's discretion.

7.27 Nowhere do the procedures make it 'extremely clear' to BOC authorised officers that, where they do not agree with the decision reached by the delegate, they cannot refuse to facilitate an override.

DIAC's procedures introduce a risk of split decision-making

7.28 In its consideration of how decisions would be made under CMAL, DIAC considered the possibility of 'split decision-making':

> If one delegate has the power to decide the entire application, but another delegate makes a decision in relation to one criterion, the first delegate may be

[243] DIAC, ibid.

[244] DIAC, *Override MAL Status*, (internal procedural instructions), 24 August 2007. These instructions are directed only to the BOC and do not form part of the PAM3 policy and procedural manual.

said to be acting under the dictation of the second. A decision in which split decision-making has occurred may be affected by a jurisdictional error.[245]

7.29 Part of the current DIAC instruction for BOC officers reads:

> A DIAC Decision Maker who wishes to override the MAL Status of a client with a high risk alert reason code may do so only in consultation with the BOC (p. 8). A Decision Maker viewing a Red MAL Status of a client with a high risk alert reason code sees the following screen in CMAL … The PAL record's biographical details and document details will display. Alerts and narratives will not display; they are visible only to BOC staff.

7.30 This text is followed by a note which, in part, reads:

> if the narrative and Case Notes do not indicate a clearance or advises against a grant (e.g. citizenship) the Decision Maker will need to be advised accordingly.

7.31 This procedure suggests that information relevant to the decision (the narrative) is concealed from the delegate. This may give rise to 'split decision-making', where an officer in the BOC is making the decision as to whether the applicant meets the criterion to which the MAL data relates.

Conclusion—a ministerial direction could be of benefit

7.32 The risk of DIAC granting a visa without first conducting a MAL check seems slight. However, DIAC regards performing MAL checks as an essential part of border protection. This suggests that DIAC should seek a remedy for its current inability to *require* delegates to check MAL. A remedy could take the form of the preparation of a new ministerial direction under s. 499 of the Migration Act. This would bring its current practice and its legal framework into harmony. DIAC has agreed to consider this course of action.

[245] DIAC, ibid.

8. Assessing MAL's performance

This chapter considers how DIAC assesses the performance of MAL, both in terms of helping DIAC achieve its outcomes and the management information DIAC gathers about MAL's use to assess the effectiveness of the system.

The value of performance and management information

8.1 Although MAL can be correctly characterised as an administrative tool rather than a program with a specific output, it has a substantial profile of its own. Given that DIAC refers to MAL as 'the department's primary tool for protecting the country from those people who may pose a serious threat to the Australian community' it is reasonable to expect that the value specifically added by MAL be capable of being distinguished.[246] That is, it should be possible to record and report its performance. Only then can government be properly informed so as to be able to decide among various options for any future changes to border protection arrangements. Sound performance information also provides transparency and accountability.

8.2 To enable management to operate a system like MAL effectively requires internal management information reports both at a day-to-day level and longer term. These enable management to monitor workloads and quality, and plan and manage changes.

8.3 The ANAO sought to identify:

(1) the performance information available on MAL; and

(2) the management information available on MAL.

8.4 At the outset, it should be noted that DIAC's latest PBS and *Annual Report 2007–08* contain no performance information specifically related to MAL.

[246] See <http://www.immi.gov.au/managing-australias-borders/border-security/systems/mal.htm> [accessed 7 May 2009].

(1) Assessing MAL's performance

8.5 The 2005 Budget papers described MAL thus:

> MAL is an electronic alert system and one of the methods the Government employs to prevent entry into Australia of people of concern.[247]

8.6 This identifies the obvious measure: the number of people of concern that MAL helps DIAC to deny entry to Australia. However, as Sadleir pointed out, there is a balance to be achieved in the design of entry control between minimising delays at points of entry and denying entry to those liable to harm the Australian community or otherwise unacceptable. It would be easy to exclude the latter consistently if the decision instrument were a blunt one, the checking processes were onerous and there was a concomitant high risk of denying entry to many travellers of no threat to the community. This would have an adverse effect on tourism and migration. On the other hand, over-preparedness to facilitate entry risks light scrutiny that allows admission of people who pose a threat to the community.[248]

8.7 Conceiving MAL in this way requires performance measures showing both how it adds value in preventing entry of people who pose a threat and the extent of inconvenience or discouragement caused, if any, by additional checking, travel delay or other negative consequence of MAL's deployment. Thus, any substantial assessment of MAL could include:

- the frequency or number of occasions where MAL has alerted DIAC decision-makers to adverse information (true matches) where that information has been used in decision-making;
- the frequency or number of occasions where that information has been a reason for an adverse decision; and
- for completeness, it could also include an indicator of how much inconvenience or discouragement has been endured by travellers as a result of delays or misidentifications triggered by MAL.

[247] Australian Government 2005, Budget Paper No.2, Budget Measures 2005–06, p. 90. See:<http://www.budget.gov.au/2005-06/bp2/html/index.htm> [accessed 7 May 2009].

[248] Sadleir Review, p. 11.

Reviews have emphasised MAL's importance but without reference to its effectiveness

8.8 Each of the major reviews of MAL has made assertions that imply the reviewer's confidence that the system is working. However, with the partial exception of the Wheen Review (see box, below), none has presented any specific performance information in support of that position. The Wheen Review concluded that 'there is a need to improve reporting arrangements' and found that 'the inadequacy of current management reporting available presents the department with unacceptable risks.'[249]

MAL performance as reported in the Wheen Review

In 2001–02, MAL produced 1.09 million notifications of possible matches resulting in 606 true matches, 227 onshore and 379 offshore. A further breakdown was not available for onshore cases. Offshore cases resulted in 61 ETA and 25 other visa cancellations. For the remaining 293 true matches the MAL records required updating or deletion.

Corresponding data for 2002–03 was that 1.34 million notifications yielded 422 true matches for offshore cases. No data was available for onshore cases. The offshore true matches led to 37 ETA and 23 other visa cancellations. The remaining 362 true matches were for cases where the MAL record needed updating.

Parliamentary committees have raised questions on MAL's performance

8.9 On several occasions in recent years, parliamentary scrutiny of DIAC's work has raised questions relating to MAL's performance in preventing entry into Australia of visitors who pose a threat:

- In February 2006, before the Joint Committee of Public Accounts and Audit, DIAC was asked about the visa application process and how many persons wishing to come to Australia would be detected in the visa checking process and fail to get a visa. In particular, the Committee

[249] Wheen Review, p. 93, para. 19.2.

made the point 'if we do not know whether people are failing or not then we have no way of saying there is a checking process.'[250]

- In April 2007, the Chair of the Joint Committee on Intelligence and Security expressed 'amazement' to read that DIAC [*then*] had 550 000 people of concern on MAL and asked DIAC, in respect of terrorist suspects, roughly how many visas had been rejected in recent years.[251] When DIAC advised that the numbers were 'quite small … of the order of maybe 10 or fewer a year' the Chair asked how that compared with people with criminal records. DIAC advised:

  > Some of that data is quite hard for us to pull out simply because of the way our own systems report. That is actually a number that I have been chasing for a while. I do not have it, but it would probably be in the 50s ... .

8.10 Although DIAC has provided data on matters such as numbers of refusals and grants on character grounds[252] it has not provided any data relating specifically to MAL's performance.

DIAC needs to keep more performance data

8.11 The audit has identified only one occasion where a DIAC document has reported along the following lines: 'There were a total number of 107 MAL matches that resulted in visa cancellations for the programme year 2004–05.'[253] DIAC keeps no regular performance information of this sort. This means that although DIAC can regularly report results to which MAL may have contributed (such as visa refusals made on character grounds), it cannot say how many of these occurred after MAL brought relevant information to attention.

8.12 DIAC has difficulty in extracting certain relevant data items from its records. Because MAL is perceived as a decision-support tool for work done with client systems, it does not receive feedback from those systems and does not hold data which shows whether it contributed to an adverse outcome.

[250] Hansard, Joint Committee of Public Accounts and Audit, (Reference: *Further inquiry into aviation security in Australia*), public hearing, Monday 27 February 2006.

[251] Hansard, Joint Committee on Intelligence and Security, (Reference: Inquiry into the terrorist organisation listing provisions of the Criminal Code Act 1995), public hearing, Wednesday, 4 April 2007.

[252] See, for example, DIAC, letter from Deputy Secretary Correll to the JCPAA, 6 April 2006.

[253] DIAC, Central MAL Metrics Report, circa December 2006. The context suggests that this figure encompasses onshore and offshore cases derived from all processing systems.

8.13 Similarly, for applications for Australian citizenship, DIAC could assess MAL's performance by reference to citizenship decisions where MAL has alerted the decision-maker to adverse information. DIAC has no data on this and advised that it would have to review each case to work this out.[254]

If MAL's successes are not assessed, its failures will be

8.14 It is important to DIAC that public confidence in its border security systems be maintained. However, while it does not count MAL's detectable successes, there will continue to be a propensity for its failures to be pointed out. This has long been understood within DIAC. For example, an internal DIAC MAL working group met after the Gerlach Review (2000) and noted:

> but what is not addressed [*in the Review*] is how we really tell when MAL is working well. *In the past we have assessed the effectiveness of MAL on the basis of failure.* Given the importance of MAL, there should, ideally, be alternative performance related assessments [Emphasis added].[255]

8.15 Similarly, DIAC's internal audit of MAL noted that: 'Because so much reliance is placed on MAL as a first line of defence, cases where someone was not prevented from entry are more readily remembered than the times that entry was prevented.'[256] Moreover, conspicuous MAL failures have been a source of contingency for DIAC. The Sadleir Review, in 1998, was triggered by failing to identify a convicted hijacker and kidnapper.[257]

How DIAC can assess MAL's performance

Numbers of matches are not a good surrogate measure of MAL effectiveness

8.16 It is worth considering whether the number of matches—particularly, the number of true matches—made by MAL is a useful measure or surrogate measure of MAL's performance.

8.17 Only by producing matches does MAL help directly to prevent persons who pose a threat from entering the country. But operational information on the number of possible matches may, at best, provide only a proxy indicator of

[254] DIAC, email advice from Director, Citizenship Operations and System Support, Citizenship Branch, 24 June 2008.

[255] DIAC, MAL Working Group, minutes of meeting, 13 June 2000.

[256] DIAC 2003, Internal Audit and Risk Management Section, Review of the Movement Alert List in a Business and System Context, February, p. 9.

[257] This matter was canvassed extensively before Senate Estimates hearings in August 1997. See Senate, Legal and Constitutional Legislation Committee, 21 August 1997, p. 69 et seq.

how MAL is performing from an external perspective. A higher number of possible matches can be produced if, *ceteris paribus*, MAL's matching algorithms are poorly 'tuned'. The number of possible matches can also be varied at management discretion by adjusting the match threshold on a risk basis. Thus the number of possible matches—although of value to management because of the workload implications—is not a useful measure of MAL performance at an outcome level.

8.18 The number of *true* MAL matches is also a potential guide to MAL's performance. Whereas only a proportion of true match cases will be decided adversely to the client, if that proportion does not vary greatly this number might still serve as a proxy indicator. However, DIAC's internal audit report of 2003 shows that the most frequent category among the true matches being made at that time is a health reason, comprising nearly half:

> The detail behind the onshore statistics revealed that all except two of the matches resulted in either a MAL record being deleted or updated. One visa was cancelled and another was identified as granted in error.[258]

8.19 The underlying issue was the lack of currency of MAL records. This is precisely the same situation as that reported above in the later Wheen Review where the great majority of true matches result in the MAL record needing either to be updated or deleted. Thus true match data could not be used directly as a proxy indicator of performance at the outcome level.[259] As DIAC is still addressing MAL data quality it is safer to assume that this remains true.

There is a need to identify where MAL has had some detectable effect

8.20 The JCPAA argument that 'if we do not know whether people are failing or not then we have no way of saying there is a checking process' is compelling. Where a DIAC officer (either onshore or offshore) has decided a visa application and MAL has drawn adverse information to their attention it should be possible to identify in DIAC records:

(1) whether the officer has had regard to that information. This is where a possible match has been identified as a true match and the information in MAL or referenced by a MAL narrative has been drawn to the delegate's attention to help their decision;

[258] DIAC 2003, Internal Audit, Review of the Movement Alert List in a Business and System Context, February, p. 16.

[259] Such use might also add weight to the incorrect notion that being on MAL, of itself, prohibits a visa grant.

(2) whether a visa application was refused or existing visa cancelled; and

(3) whether information provided by or drawn to attention by MAL was the reason or part of the reason for refusing or cancelling the visa.[260]

8.21 A count of instances that satisfy all these conditions would be a count of the persons who have 'failed the checking process' because of MAL.

Numbers of visas cancelled where MAL has contributed information

8.22 A further measure could be of cases where a visa is cancelled as a result of adverse information identified through MAL. After full CMAL implementation it is likely that this will happen much less frequently than visa refusals.[261] For example, it could occur where new information entered into MAL is checked against visas already in effect and attracts a true match.[262]

Facilitating an approximation to 'visa-free' entry

8.23 A substantial beneficial effect of MAL is its use in underpinning the development of the ETA. Enforcing rigorous entry and stay provisions while maintaining a universal visa system has only been possible because of MAL. All ETA visitors have, in this sense, had their visit to Australia facilitated by MAL. It may be possible to derive a measure of the number of cases of entry facilitated by MAL, as a counterpart to cases where entry has been prevented.

8.24 Further, through facilitating the development of the ETA and other visa types that can be electronically granted,[263] MAL has indirectly helped to influence other countries to allow visa free entry to Australians. MAL facilitates reciprocal visa-free arrangements with other countries at a time when those countries are competing to lower unnecessary entry constraints to promote inbound tourism. However, there is no obvious way of measuring this benefit.

[260] It must be possible to identify such cases. If it were not, it would not be possible for DIAC to satisfy s. 57 of the Migration Act, which explicitly requires the minister to give relevant information (other than non-disclosable information) to an onshore visa applicant where that information would be the reason or part of the reason for refusing to grant a visa. However, it may still be resource-intensive and a sample-based approach may be necessary.

[261] Before full CMAL implementation MAL checking in offshore visa grants used a less sophisticated suite of matching software. This means that some true matches were identified after visa grant, when the better software was applied at visaload. After CMAL implementation such cases should be identified at the visa grant stage. Thus, after CMAL implementation, the number of visa cancellations ultimately due a MAL true match should tend to decline and the number of refusals should increase.

[262] DIAC advised that MAL has no role in citizenship revocation. (Advice of 22 January 2009).

[263] This includes visas such as the Working Holiday Maker visa (subclass 417) and e-676 tourist visa.

'Missed' cases

8.25 Another useful measure could be of the frequency with which DIAC later discovers that MAL failed to detect a person on whom it held adverse information before issuing a visa or admitting them into the country. That would state, in effect, how many people are later discovered to have been missed by MAL checking or where that checking was not properly discharged. This could include those to whom DIAC granted a visa or citizenship before all normal checking procedures had been completed.

8.26 Current practice is that the CMAL Operations Section reports urgently to a deputy secretary where it later discovers a miss of a *National Security* case. Further, DIAC has prepared detailed lists in the past of missed cases, setting out the details, a chronology of events and the reasons for the miss having occurred.[264] This could be a concomitant to the measure of the numbers prevented from entering. However, if it were regarded by competent authorities as not in the national interest that this inherently sensitive information be reported publicly, it could be reported to the minister.

Inconvenience to travellers

8.27 DIAC advises that, to minimise inconvenience in cases of travellers having similar biodata to a MAL listed-person it addresses these circumstances on an individual basis.[265] It has recognised that CMAL contributes to client convenience:

> While largely aimed at strengthening border security, [CMAL], once fully deployed, will also improve client service by reducing the requirement for multiple MAL checks to be undertaken and minimising the need for post-visa grant intervention due to MAL issues.[266]

8.28 It might, therefore, be useful to measure the adverse effects of MAL, such as delays experienced by genuine travellers as a result of MAL checking. CMAL is likely now to be improving DIAC's client service but the department does report any specific or expected improvements. An indicator for a substantial proportion of cases may be the time taken to resolve potential MAL

[264] Separate lists were prepared of missed matches in *National Security* and non-*National Security* cases during 2006–07.

[265] DIAC advice of 22 January 2009.

[266] DIAC, *Annual Report* 2007–08, p. 94.

matches for ETA applications.[267] CMAL will have lowered inconvenience to travellers by reducing the proportion of cases referred to the nearest post.[268]

8.29 The ANAO suggests that DIAC consider whether it could usefully report on:

(a) the numbers of cases where MAL is found to have missed a case; and

(b) inconvenience to travellers and citizenship applicants caused by MAL checking.

Conclusion—more could be done to measure MAL's performance

8.30 On a number of occasions it has been apparent that DIAC has no information that shows how successful MAL is in helping it to achieve its outcomes. DIAC produces no data of this kind.

8.31 In administering a key business system, such as MAL, a balance should be struck between the cost of collecting performance information and the benefits to DIAC and key stakeholders, such as the Parliament, of this information in demonstrating MAL's successes. In this context, sound performance information would include data on DIAC's success in using MAL to (i) prevent people from entering Australia who pose a threat to the community and (ii) prevent such people from getting Australian citizenship. The range of other measures identified in the chapter could also help DIAC gauge the value being added by its use of MAL.

[267] Presumably this could be calculated by measuring the time taken to resolve each potential match and taking the mean and reporting this figure, say, monthly.

[268] Prima facie, ETAS statistics provided by DIAC show that 8.5 per cent of ETA applications (of which there were about three million) were referred to post during the 2006–07 financial year. Figures for the first few months of CMAL operation for the ETAS environment show that under half of one per cent of cases were referred to post. This should also have substantial benefits for the workload at posts. DIAC has reported that the numbers of cases referred to posts are much reduced after the introduction of CMAL for ETAS, but does not state the magnitude of the reduction, nor the time taken to resolve matches. See DIAC, *Annual Report* 2007–08, p. 50.

Recommendation No.3

8.32 The ANAO recommends that DIAC improves its reporting on the performance of MAL by, where practicable, identifying instances where MAL has alerted its decision makers to information that has been the reason, or part of the reason, for decisions on visa and citizenship applications.

DIAC response: *Agreed*

> DIAC agrees to this recommendation, noting that the new CMAL system provides, for the first time, an opportunity to maintain comprehensive information on actual true matches between the database and DIAC clients. We intend to regularly sample such true matches and track through the decision-making process to determine what role MAL information has played in the visa decision. It should be noted that, because MAL is advisory information only, the actual visa decision outcome cannot be expected to be adverse in all cases, and in some cases the role played by MAL will be difficult to quantify or differentiate from other factors. In many cases, review of the MAL information by the decision-maker will lead to the conclusion that visa grant is acceptable. This information will be used internally to refine practices and procedures and generate greater awareness of the role that MAL can play in decision-making.

(2) Management information on MAL is limited

8.33 The ANAO examined DIAC's arrangements for providing management information on the performance of MAL. Even though, as concluded above, there is no current mechanism for reporting MAL's overall performance, there are indicators of value to management that could be reported.

8.34 Specifically, the ANAO examined:

- whether DIAC had identified performance indicators it required;
- whether it recorded and reported against these; and
- whether there remain opportunities from improved reporting.

8.35 MAL operations in recent years have been dominated by the CMAL project. This has performance parameters of its own that management needs to measure to monitor progress. The focus here is on MAL performance in a general and ongoing sense: CMAL is discussed in the next chapter.

DIAC has identified useful performance indicators

8.36 The earlier reviews of MAL have focused on a need for better reporting to help management of MAL itself. In 2000, the Gerlach Review reported that:

> The only reports available in MAL are lists of all PAL or DAL records. Two additional statistical reports have been developed in the last months: one to list the number of records in PAL by risk category and by the number of poor biodata records; and another to list provide [sic] a statistical report of the match rates for each different business rule, by risk category. This gives an overview of how MAL is performing.[269]

8.37 This review recommended that a suite of additional reports be developed, including numbers of true matches. The internal audit (2003) also recommended that DIAC produce a quarterly statistics report for senior management.

8.38 The Wheen Review was more comprehensive and made two specific recommendations about reporting on MAL performance. The first proposed that, as a priority, DIAC develop a reporting strategy for MAL to 'meet the requirements of operational management, system management and senior management.' The second proposed that reports have a broad coverage 'to include not only timely information about systems operation but include data quality, provide a quality assurance perspective and address training delivery.[270] The MAL Review Team concluded:

> Reporting on MAL operations to all levels of management on MAL operations is seriously deficient and the inadequacy of the management reports available from MAL presents unacceptable risks to [DIAC]. A plan needs to be put in place as a matter of urgency to deliver a suite of relevant reports.[271]

8.39 A copy of the Wheen Review's proposed reports on MAL performance is at Appendix 4.

[269] Gerlach Report, p. 33.

[270] Wheen Review, p. 93.

[271] Wheen Review, Appendix 2, Deliverable B9.

DIAC has some performance information on MAL but does not report it

8.40 DIAC's current performance reports on MAL[272] primarily provide data on the following parameters:

- numbers of PAL records (by Alert Reason) and numbers of DAL records;
- numbers of MAL notifications (that is, possible MAL matches identified by the system);
- numbers of MAL referrals (that is, likely MAL matches forwarded to a responsible business area/external agency for confirmation); and
- approximate numbers of true matches and non-matches, outstanding matches; matches on hold.

8.41 DIAC has also produced other reports from time to time. For example, during the six months or so after initial CMAL implementation (October 2007), DIAC produced a report on its backlog of CMAL match cases, by priority. This helped it to manage the resolution of processing backlogs (see Chapter 8).

There are opportunities for improved performance reporting

8.42 The material currently being produced reflects many of the items set out in the Wheen Review's 'General' category. The obvious exception is 'Nos of visas which result in a true match x alert code x subsequent action taken', which takes us to the outcome of the process, a matter discussed in the earlier part of this chapter.

8.43 Other opportunities to improve reporting on MAL relate to:

(1) data quality of new entries;

(2) client service standards; and

(3) overall system reliability.

(1) Data quality of new entries

8.44 As DIAC advised at the commencement of the audit, the quality of entries in MAL has been a long-established challenge to optimising MAL's

[272] There are three regular reports: Border Security Division (BSD) Executive Monthly Statistics; BSD Senate Estimates; and BSD Performance Assurance Report (quarterly).

operation. Each review of MAL has argued the case for working to improve the quality of the data (see Chapter 2). The Wheen Review had specific suggested proposals for reporting on data quality.

8.45 Given that improving data quality remains a desirable objective it would be useful if some measure were made of new data being entered into MAL and this were reported regularly. For example, it could measure and report, each month, the proportion of records, by Alert Reason, that satisfy its expectations for completeness. A focus on new data, especially on that sourced within DIAC, would give some sense of progress being made in adopting sound practice.

(2) Client service standards

8.46 DIAC advised at the start of the audit:

> Client Service Standards are governed by the various Posts/STOs in liaison with National Office Policy Areas. CMAL Operations work closely with stakeholders to ensure expectations are met. A review of our performance standards is being assessed.

8.47 DIAC's planning documentation shows that the model it has derived from this review maps each of about 180 different case types into one of 11 different service level categories with a required resolution time (service level) of between two hours and 15 days.[273] For example, DIAC expects possible matches for ETA cases to be resolved within 12 hours.[274] To help deal with the complexities of allocating match resolution work to best meet expected service levels, DIAC proposes to introduce a work allocation system in a future *Systems for People* release.

8.48 The planning documentation states that it is not possible to monitor and report on service level attainment under the current work allocation system. However, this will be possible under the intended changes.

8.49 DIAC subsequently advised that:

> CMAL has put in place a Service Level Agreement for the client service network and this forms the basis for match case processing priorities. The CMAL Operations Section will report against this periodically to the service

[273] DIAC, SFP031-D, Central Movement Alert List (CMAL) Project Implementation Plan, SFP8, 16 October 2008.

[274] This 12 hour standard does not apply in the small proportion of cases that are referred to a security agency for clearance.

delivery network and seeks feedback on unique issues with respect to the delivery of services.[275]

8.50 The department also added that 'System and processing reliability is more visible under the CMAL capability.' When a stable operating environment for CMAL has been achieved, data on actual performance against these standards will be important to aid effective ongoing management.

(3) MAL reliability

8.51 Like any major, complex system, MAL is subject to potential failure, if only in parts of the system. During the course of the audit the ANAO identified three separate and apparently independent incidents affecting parts of MAL all of which persisted for months before coming to management attention and being addressed. With MAL being a central element to border protection, it is important that DIAC management have mechanisms in place to provide assurance that all parts of this increasingly complex system are operating satisfactorily, from an 'end-to-end' perspective. That is, when a failure in some part of the system occurs, it should be promptly identified and brought to management attention for corrective action.

8.52 The incidents which came to the ANAO's notice were:

- a corruption of the Entry Control Point MAL check;
- a failure to update the Customs and Border Protection copy of MAL; and
- a failure to copy all MAL records when creating DIAC's 'MAL Contingency Database'.

Corruption of the ECP MAL check

8.53 In November 2006, the MAL check process at the primary line for clearance of passengers entering Australia at airports and seaports ceased working properly for about six months.[276] MAL continued to carry out its other major functions satisfactorily, such as checks performed for visa processing and at the visaload process, during this time.

[275] DIAC advice of 9 March 2009.

[276] At international ports, initial contact with disembarking passengers seeking to enter Australia is made by Customs and Border Protection at the primary line. Passengers triggering customs, quarantine or other alerts are also identified at this time.

8.54 The MASC project—to upgrade the name matching software—was implemented in November 2006. The implementation seemed to go well and a project closure report was signed in March 2007. However, it had escaped DIAC's notice that a program module had not been put into production and, as a result, the Entry Control Point[277] MAL check process (invoked by the Customs and Border Protection system, PACE) was corrupted so severely that it ceased working properly. This meant that virtually no match results were returned from the time of implementation until the problem was addressed in June 2007.[278]

8.55 DIAC carried out a post-implementation review (PIR) to:

- identify the scope of cases not properly MAL checked; and
- identify lessons learnt and provide recommendations for improvements to reduce the risk of such a problem re-occurring.

8.56 DIAC has subsequently advised that all clients processed through the ECP MAL check were at all times subject to the [later] visaload MAL check: 'Post-incident reconciliation by the MAL Operations Section discovered no cases where clients had remained without a MAL check, and no actual MAL matches.' The department also advised that the ECP MAL check is used only to process a small number of low risk passengers.

8.57 The PIR concluded that:

> The fault with the ECP MAL check went undetected for more than 233 calendar days because the MAL check processes operate as a 'black box' and there is very little scope for the end user to assess whether it is returning sound results.[279]

8.58 The PIR recommended, *inter alia* that DIAC:

> - Develop a MAL health check 'scorecard' for all critical MAL business functions. The 'scorecard' entries should be supported by automated processes wherever possible.

[277] Entry Control Point (ECP) is the system that interfaces with Customs and Border Protection's PACE system for processing travellers' movements to and from Australia. ECP collects transactions, loads them into the mainframe, checks and confirms data before sending it back out to PACE and other linked systems.

[278] DIAC, *Post Implementation Review of the MAL SNAPIS/Software Upgrade Project (MASC001) in relation to the corruption of the ECP MAL Check process that occurred from the 30 November 2006 to 19 June 2007*, 24 September 2007.

[279] The PIR also gives the period as 210 days at another point.

- Conduct regular system health checks to monitor the integrity of all critical MAL processes.

Failure to update the Customs and Border Protection stand-alone copy of MAL

8.59 As mentioned earlier, DIAC provides a copy of MAL to Customs and Border Protection. In March 2009 DIAC advised that it had discovered that the Customs and Border Protection copy of MAL had not been updated properly for some 13 months. It provided the following account of the incident:

> On 10 February 2009 DIAC encountered a network virus and the ECP linkage with Customs was affected. Customs operated in fallback mode on 10 and 11 February relying on their (stand-alone) copy of MAL to match travellers rather than on the DIAC expected movement records with an immigration directive. This copy of MAL is updated by an hourly batch file transfer from DIAC.
>
> On 12 February 2009 Customs advised DIAC that following the re-establishment of the ECP linkage they noticed that the regular batch file transfer of MAL updates sent from DIAC contained only nine records and that all batch transfers since 21 January 2008 had contained the same nine records. Effectively, the Customs version of MAL had not been updated since 21 January 2008.
>
> It is important to note that the Customs version of MAL is only used to check travellers during periods when the ECP linkage between DIAC and Customs is inoperative, such as during scheduled mainframe outages in DIAC or unscheduled system downtime in either DIAC or Customs. There are monthly scheduled outages in DIAC's mainframe environment.
>
> In addition, in these times of system outages, Customs use their stand-alone version of MAL, and passengers continue to be MAL checked at time of visa grant and/or passport or visa loading, through the Advanced Passenger Processing system at airline check-in and again after actual movement records are transferred to DIAC. As a result, the risks are extremely low.
>
> DIAC has undertaken a reconciliation of passenger records for the full period that the batch file transfers were not updating correctly and found movements for 16 persons with possible matches against DIAC's current version of MAL where the corresponding MAL record was created or updated during the outage period. Investigation of these cases has revealed no true matches against the DIAC copy of MAL.
>
> DIAC is working actively with Customs to bring their stand-alone copy of MAL up to date. However, while DIAC is able to provide all missing updates, there are technical issues affecting Customs' ability to update their copy. Business areas are assessing the need for use of manual procedures during

> times of outages (scheduled and unscheduled) to the ECP link in the interim period while this issue is rectified.
>
> Again it should be noted that the transient risk of missed matches is quite small (as demonstrated by the reconciliation), and is further reduced by the operation of CMAL in the Visa, APP, and TRIPS Referrals systems, before and after arrival.

Failure to copy all MAL records when creating DIAC's 'MAL Contingency Database'

8.60 DIAC's CMAL Operations Section regularly produces copies of the MAL database called the 'MAL Contingency Database'. This is available for reference in the Border Operations Centre in the event that the mainframe is unavailable. DIAC has used this copy of the data each month to create its monthly MAL statistics. However, the audit led to the discovery in July 2008 that the MAL Contingency Database had been incomplete for some months.

8.61 When DIAC provided a copy of the MAL database to the ANAO in the course of the audit it drew that copy from its MAL Contingency Database. However, the ANAO observed that records it could access on the live copy of MAL, on the DIAC mainframe, were absent from the copy provided for audit analysis. Upon investigation, DIAC reported that this anomaly flowed from an error in updating the MAL Contingency Database.

8.62 DIAC advised that the problem with the MAL Contingency Database was 'not limited to just a few records' but all Alert Reasons with a particular transaction type:

> As a result of this error, some PAL records whose details are updated in Mainframe MAL would never be reflected in the MAL Contingency Database, thus creating a difference between what is visible in HMAL production and the MAL Contingency Database.[280]

8.63 This means that:

- if DIAC had needed to use the MAL Contingency Database it would then have had access only to an incomplete set of records. The number of missing records is not known but was probably very few; and
- the MAL statistics generated from the inception of the fault until February 2008 (when a different method of generating them was

[280] DIAC, email advice of 7 July 2008. The ANAO understands that the error affected any MAL record that was updated within 30 minutes of having been created.

adopted) are incorrect, though it is unlikely that they are substantially so.[281]

8.64 DIAC advised that the problem had been introduced at CMAL implementation in October 2007.[282] After correcting it, DIAC provided the ANAO with a new, complete copy of the database, which formed the basis of all the analyses in this report.

8.65 The common issues among the three incidents discussed above are that:

- each continued for an extended period (from six to thirteen months); and
- DIAC management became aware of them only fortuitously rather than by any systematic method of assurance.

8.66 DIAC has advised that regular running of a number of reports and measures it has in place should have highlighted, at an earlier time, both the ECP MAL module problem and assisted with earlier recognition of the problem in updating Customs and Border Protection's copy of MAL. However, the department advised that 'it appears that these reports have not been run as regularly as they could have been'.[283]

Conclusion—management information on MAL is limited

8.67 Management information on MAL is limited. It would help DIAC to manage MAL better if it were to measure and report internally on data quality, client service, and overall system reliability.

8.68 DIAC has suffered a number of failures in parts of MAL and each of these has remained undetected for an extended period. Although there is no evidence that any of these incidents has resulted in any inappropriate admissions into Australia, the department needs to have a mechanism in place that will draw such incidents to attention promptly in future.

[281] DIAC advised (21 August 2008) that: 'Figures produced between October 2007 and February 2008 for number of records on PAL and number of records on DAL may have been affected by the recently rectified Contingency problem. It is not possible to state the magnitude of the problem.'

[282] DIAC, email advice of 21 August 2008.

[283] DIAC advice of 19 March 2009.

Recommendation No.4

8.69 To enable DIAC to manage MAL effectively, the ANAO recommends that DIAC seek to measure and report internally on:

(a) data quality;

(b) MAL's reliability; and

(c) client service, measured by the service level agreements agreed internally with CMAL client areas of the department.

DIAC response: *Agreed*

(a) DIAC agrees to the further development of measures to determine the overall usefulness of the information contained within the MAL database. The need to accept some records that do not meet all data standards will be better managed in future with the implementation, in March 2009, of the new Remote Input Function (RIF) in CMAL, which provides for all new records to be reviewed by CMAL match analysts before entry into the database.

(b) DIAC already has an established process of reporting on and responding to service outages in IT systems. Under this system MAL and CMAL outages are rated as 'Severity 1' and responses are undertaken with the highest priority. Noting the incidents discussed by the ANAO in the course of the audit, DIAC agrees that reporting on separate MAL-related issues and operational functionality can be accorded separate focus. DIAC has already instituted monitoring that will provide more timely alert of interruptions to MAL services provided to the Australian Customs and Border Protection Service, while CMAL will also be subject to regular monitoring and monthly reporting on planned and unplanned service interruptions, their causes and solutions. DIAC will also continue to undertake post-incident investigations to provide assurance that border and visa integrity have not been compromised by such incidents.

(c) DIAC has already implemented monthly reporting on achievement of the Service Level Agreement negotiated with the DIAC Service Delivery Network.

Recommendation No.5

8.70 The ANAO recommends that DIAC implements a mechanism for providing regular assurance that all key parts of the MAL system are operating satisfactorily.

DIAC response: *Agreed, noting the measures advised under Recommendation 4(b).*

9. CMAL implementation

This chapter examines whether DIAC has implemented CMAL in accordance with its proposal in 2005, as agreed by government at that time.

DIAC identified a need to upgrade MAL

9.1 The 2003–04 Budget funded a proposal from the then Immigration Minister 'to establish a task force to determine the optimum means of implementing the next generation of MAL, which will operate in real time and support new identification technologies'.[284] That task force became the Wheen Review, whose principal outcome has been the CMAL project.[285]

The risks of not upgrading MAL

9.2 DIAC developed a new policy proposal to fund a project to implement the Wheen Review recommendations. As part of this, it prepared a business case whose foundation was improving the effectiveness of MAL rather than any change in efficiency.[286] The essence of the proposal was this:

(1) Although it is not possible to eliminate all risk of failing to identify an individual or document about whom MAL holds information, the risks inherent in MAL's operation had become 'significant'.

(2) The Wheen Review had identified two major risks:

(i) the weaknesses of the name matching software used in DIAC's offshore processing systems; and

(ii) the fact that possible matches were assessed by many hundreds of DIAC staff across the department. These staff were inexpert in the name-matching task, often focused more on facilitating entry than border control and had become reliant on the 'safety

[284] DIAC, minute from the Executive Co-ordinator, Border Control and Compliance Division, to the Minister for Immigration and Multicultural and Indigenous Affairs, 17 September 2003.

[285] The review was originally expected to be complete by 30 April 2004. In the event, DIAC advised the minister in August 2004 that the MAL Review had now been completed. (DIAC, minute from the Executive Co-ordinator, Border Control and Compliance Division, to the Minister for Immigration and Multicultural and Indigenous Affairs, 27 August 2004.)

[286] DIAC, 'Responses to questions regarding the Central MAL Project asked by Finance 15 Feb 05.'

> net' provided by the second round MAL check after the visa had been granted to pick up what they missed.[287]

(3) The risk was more acute because of:

(i) a perceived increased threat to Australia from international terrorism since September 2001; and

(ii) rapidly rising numbers of records being added to MAL, in particular, high-risk records of people of security-related concern. This was changing the balance in MAL's functions from its original immigration focus to a greater security focus.

9.3 The Business Case concluded that, without a major investment in MAL:

> the Government would face some difficult options. The volume of alerts would lead to a need to lift [*the match threshold*] so that the system did not present so many alerts to staff. The risk to Government of genuine matches being missed would become higher and higher.

The Wheen Review set the way forward

9.4 The Wheen Review had considered a wide range of matters in the design and operation of MAL. The report included 63 specific recommendations, all of which were included in the policy proposal agreed and funded by government in the 2005 Budget.[288] The Budget papers explained:

> This measure implements key recommendations of the 2004 Review of the Movement Alert List … [*including*] creating a 24-hour onshore processing centre,[289] redeveloping associated IT systems, establishing secure means of communicating with overseas posts and regional offices in Australia, and facilitating the secure exchange of electronic data between [DIAC] and ASIO.[290]

9.5 DIAC was implementing major stages of CMAL during the fieldwork for this audit in 2008. The implementation has brought a substantial change to operations with the redevelopment of an important IT system. However, over recent years other, other changes with a high IT component have also been

[287] DIAC, ibid., p. 3. The 'second round' check was what DIAC calls the 'visaload' process, when details of visas granted are subsequently entered into DIAC's TRIPS system.

[288] The 2005 Budget was brought down on 10 May 2005.

[289] 'CMAL'—'Central MAL'—reflects the centralisation of MAL matching operations in DIAC's national office.

[290] Australian Government, Budget Paper No.2, Budget Measures, p. 90.
See: <http://www.budget.gov.au/2005-06/bp2/html/index.htm> [accessed 7 May 2009].

under way in DIAC. The *Systems for People* (SfP) project has brought department-wide systems-based reforms many of which derive from the Palmer Report and subsequent related work.

9.6 Although DIAC now attributes the changes brought by CMAL to SfP,[291] CMAL has an earlier and distinctly different point of origin, and was separately agreed to and funded. CMAL has been embraced within the SfP framework while retaining its identity.

9.7 To examine whether DIAC has implemented CMAL effectively the ANAO considered the following:

(a) whether DIAC identified in advance what the project would achieve;

(b) whether DIAC also stated how it would measure progress and assess its success, and whether it has done so;

(c) whether CMAL has been delivered on time and within budget; and

(d) arrangements for review of the project.

9.8 The concurrence of the audit fieldwork and major implementation phases of the project places limits on the scope of findings on CMAL progress.

(a) DIAC identified project objectives in advance

9.9 Only by identifying specific project objectives in advance can a project's achievement be identified in an accountable way. Objectives should therefore be stated at the outset, clearly and unambiguously. DIAC did this in various documents at various stages of the project. For example, in the CMAL Baseline Project Management Plan (June 2005), the project objectives are specified as:

- Establish a centralised onshore MAL Centre to undertake 24/7 MAL operations by well managed, trained and specialised staff including the transitioning of EOC and MAL operations to the new Centre.
- Develop and implement a single onshore MAL system upon which all visa issuing/checking programs can call to compare identity's details with the Movement Alert List. The Central MAL system will be a key element in the development of a centralised suite of Integrity Services.

[291] The DIAC *Annual Report*, 2007–08, states: 'Through Systems for People the Department has also transformed its border entry and security checking systems through the introduction of a new Central Movement Alert List (CMAL) business model' (p. 135).

- Enhance the Departmental and external agency communication links so as to securely support the above objectives.

9.10 These objectives articulate the core of the project, as can be seen by reference to the discussion of the business case (para. 9.4, above). However, they do not encompass the majority of the Wheen Review recommendations.

(b) DIAC also identified in advance how it would assess success but has not yet done so

9.11 For proper accountability, measures by which a project's level of achievement will be assessed should be set out in advance. DIAC identified two ways in which it would track and measure progress:

(1) at the outset, a specific set of performance criteria; and

(2) in late 2005, a report called 'the project sponsor's report'.

(1) The specific set of performance criteria

9.12 DIAC set out a specific set of performance criteria to gauge the CMAL project's overall success. These were part of its new policy proposal and reproduced in the 'baseline project management plan':[292]

- 50 per cent improvement in effectiveness of the MAL match process;
- 25 per cent improvement in the effectiveness of name matching processing;
- 50 per cent improvement in MAL data quality through enhanced quality assurance procedures;
- 100 per cent improvement in security of MAL data;
- 50 per cent improvement in management, reporting and strategic planning;
- 50 per cent reduction in risk of possible matches being referred to security agencies only after visa issue; and,
- 50 per cent improvement in the timeliness and accountability of visa security checking processes for both [DIAC] and security agencies.[293]

[292] DIAC, Movement Alert List (MAL) Baseline Project Management Plan, version 2.0, February 2005, p. 8. This plan was originally drafted in January 2005, preparatory to formal approval from government. The plan was refined and updated at various times during 2005.

9.13 This set of criteria presents some obvious challenges. None of the documentation reproducing setting them out explains how they were chosen nor how, when they were devised, DIAC intended to measure them.

DIAC has not yet assessed progress against the 'specific performance criteria'

9.14 The CMAL Project Manager at the time later attempted to devise a practical means of interpreting most of these criteria so that they could be measured and tracked, albeit two months after the government had agreed to the CMAL proposal, including these criteria. However, there is no evidence that DIAC attempted to do so, even when prompted by the Cabinet Implementation Unit (CIU) in the Department of the Prime Minister and Cabinet.

9.15 DIAC noted in July 2006 that it would be required to report progress quarterly to the CIU.[294] In November 2006 the CIU asked a specific question about progress against these criteria and DIAC responded:

> Is information being collected against specific performance criteria set out in [*government decision*], e.g. 50% improvement in effectiveness of MAL match process, 100% improvement in security of MAL data, 50% improvement in management, reporting and strategic planning?
>
> Answer: *No—CMAL has not yet been implemented.*

9.16 To enable it to assess the degree of improvement actually achieved DIAC should, at least, have commenced collecting baseline data against which it could subsequently compare its later position. Without that, data collected after implementation had started would be of diminished value as there would be nothing to compare it with and no basis for claiming any improvement.

9.17 Moreover, the implication of DIAC's response to the CIU is that, once CMAL implementation did begin in October 2007, DIAC would measure against these criteria. Even though implementation has been staged, each such stage could reasonably be expected to yield some improvement (and possibly some unintended consequences). There is no obvious reason why that should not be tracked. In fact, DIAC has not reported progress against these criteria.

[293] DIAC, Central Movement Alert List (CMAL) Project Quality Plan, version 1.0, August 2005, p. 5. Note: These lists of critical success factors and performance criteria are reproduced in a number of places through CMAL project and other documentation such as the Border Security Division Program Performance Requirements 2005–06, p. 53.

[294] DIAC, Central MAL Working Group Minutes, 17 August 2005.

9.18 DIAC continued to report on CMAL to the CIU in the form required by that unit until the CIU no longer required updates. However, these reports were about the project's major milestones and did not address project performance in terms of the criteria originally specified.

(2) The Project Sponsor Report: 'Our total response to Wheen'

9.19 A comprehensive mechanism for monitoring progress was devised in late 2005. The then First Assistant Secretary, Border Security Division, set out his requirements in straightforward and readily comprehensible terms:

> My approach as the project sponsor is as follows:
>
> - I commissioned the Wheen Review.
> - It identified a range of issues and made a series of recommendations.
> - We evaluated the Wheen Review and went to Cabinet to address the issues it raised. We got what we asked for and the Government then expects the issues to be addressed. We will be measured in respect of our total response to Wheen.
> - Accordingly, what I want is a report—you can call it the Project Sponsor report if you like—which sets out the Wheen recommendations and reports on each. If there are subsidiary issues raised then we need to list.[295]

9.20 From the context of the exchange in which this requirement was set out, it was clearly intended to broaden the focus of project reporting from the core objectives (as set out above, para. 9.9) to the full suite of Wheen Review recommendations. DIAC then prepared a detailed report—the 'Project Sponsor Report'—showing each of the recommendations and progress against it.

The Project Sponsor Report fell into disuse almost immediately

9.21 DIAC soon ceased using the Project Sponsor Report. The ANAO identified a version dated October 2005 (presumed to be the original) and a substantial update in February 2006. Although DIAC provided a further update in July 2008, this was prepared to meet the ANAO's request to see a

[295] DIAC, email from First Assistant Secretary, Border Security Division, to Assistant Secretary, Border Security Systems Branch, 11 October 2005.

current version of the report.[296] However, DIAC management has not been using the mechanism as a management tool over the last several years.

9.22 It is apparent from reviewing the Project Sponsor Report that certain Wheen Review recommendations which have not been implemented could have improved MAL's operation. Some of these were judged to be priorities at the time of the Review. Two prominent examples are:

- ***Recommendation 10.25:*** *A properly resourced quality assurance process be established to monitor and enhance the quality of data in MAL and that being entered into MAL.* This could have been done independently of developing the new CMAL application, setting up the BOC and so on. If a sound QA process had been applied to the data from 2005, the benefits would have substantial 'washed through' the system by now.
- ***Recommendation 19.7:*** *As a priority, develop a reporting strategy for MAL in line with the Department's overall Reporting Strategy and ensure that in designing the necessary reports they meet the requirements of operational management, system management and senior management.*

9.23 CMAL's project managers were placing at least one of these courses of action at a distance from the core project as early as mid-2005:

> - Quality of MAL records/data. Data quality is outside of the CMAL project's scope (it resides with the day-to-day business owners), but unless substantial advances are made in this area, then the number of MAL name matching staff may continue to increase.[297]

9.24 The consequences of not addressing data quality has been analysed and discussed in Chapter 2. The point here, however, is that DIAC ceased systematic tracking the recommendations of a project specifically authorised by government. Where events have overtaken some of these an appropriate course of action would have been to have reported this and acquitted the matter appropriately with advice to the minister.

9.25 Consistent tracking of progress with implementing the authorised recommendations could have highlighted insufficient progress with important measures such as the two listed above.

[296] The update provided by DIAC to the audit team in July 2008 is dated both 'July 2008' and 'Feb 2006'. It seems probable that the February 2006 edition was the latest update on which to base a July 2008 edition.

[297] DIAC, NPP Project Status Report, 2005.

(c) CMAL has been delivered late, but within budget

9.26 Most projects face unforeseen contingencies which, sometimes, cause changes to the project timetable. Well-managed projects can show evidence of reasoned consideration of the options in the face of contingencies and a rationale for any delay. There should also be evidence that those who authorised the project are advised of any major timetable changes, if not involved in major decisions.

9.27 The CMAL Project effectively started in November 2004 when DIAC endorsed the Wheen Review's findings. When the Government agreed to the project and funded it, DIAC set out the project deliverables in four phases. It intended to implement the first in December 2005 and the last, involving all processing of MAL matches by the new BOC, by September 2006.[298] It was to complete a post-implementation review by August 2008.

'Re-baselining' the CMAL project management plan

9.28 In the event, the CMAL project has been affected by contingencies that have changed the timetable considerably. The most substantial change was in mid-2006, associated with the SfP project which, although it commenced later, has an overarching nature that affects all DIAC computing.

9.29 By early 2006, CMAL's schedule was under pressure. DIAC's internal technical architecture council rejected an important project document, the technical discovery paper. The business and technical discovery processes, part of DIAC's normal system development methodology, had identified many requirements not apparent when it developed the new policy proposal. These included a need to migrate MAL from a mainframe to a mid-range processor and interdependence with the new identity services suite of facilities.

9.30 DIAC had also decided that CMAL would be a 'portal project', which meant that it must now fit under the SfP strategy. In May 2006, the CMAL Systems Application Development Manager noted that:

> A decision has been made to return to the vision and reconfirm all requirements. This is an excellent decision which will serve the project well in the long run, however in the short to medium term this will impact the project

[298] DIAC, agenda paper for IT Governance Committee meeting, 23 March 2005.

schedule. *We are effectively starting from the beginning of the development lifecycle.* [Emphasis added][299]

9.31 In essence, DIAC then found that it needed to assure itself that it had a clear idea of what the project was to deliver —the project 'vision'—and that all the requirements were correctly specified and understood. Thus, at least for the development of the new CMAL application software, this meant a return to the start. The amended timetable for CMAL to begin operation became:

- Core CMAL (January (now unlikely) or April [*2007*])
- CMAL with TRIPS and ICSE (April [*2007*])
- CMAL extended to IRIS and ETAS (July [*2007*])

9.32 'Continuing changes in management' were a further source of contingency for the project throughout mid-2006, flowing from the SfP changes.[300]

9.33 As part of the revised planning that took place at this point, DIAC also reviewed important project documents to determine which had 'status', resolving that only two did: the new policy proposal to government and the Wheen Review. This meant that only those documents could provide authoritative guidance to the 're-baselining' of the project.

9.34 DIAC drew up a new *CMAL Project Management Plan* in mid 2006, reflecting the newly-endorsed project vision. It replaced the previous 'CMAL PMP *Central Movement Alert List (MAL) Baseline Project Management Plan*, June 2005, v3.1'. Its purpose was 'to provide critical stakeholders including the CMAL project team with an agreed project definition of the re-baselined Central Movement Alert List (CMAL) project.' SfP is listed as a constraint on the CMAL project and the plan notes a 'Need to align with Systems for People projects and release schedules'.

9.35 The new plan included two other notable elements:

(1) *A 'traceability matrix'.* The new plan's authors examined both the Wheen Review and the subsequent new policy proposal to identify the scope of the CMAL project. It interprets the scope as including:

- all the specific recommendations of the Wheen Review; and

[299] DIAC, CMAL Project, Application Development Status Report, 15 May 2006.

[300] DIAC, CMAL Project, Application Development Status Report, 2 August 2006. Some of these changes included the introduction of new managers into the CMAL project employed by DIAC's strategic partner in the SfP development.

- all the other commitments introduced in the new policy proposal. This includes assessing progress by the specific criteria mentioned earlier.

In addition, the new plan identifies the DIAC functional unit responsible for each of these items.

(2) As part of the traceability matrix, the plan identifies some items (some 17 from the review and three from the NPP) funded by the CMAL project but out of scope of the core IT project.[301]

9.36 The new plan was submitted to DIAC's Border Systems Board for endorsement in July 2006.[302] Among the reasons given for the change were that 'the department's new strategic partner would need an up-to-date and endorsed CMAL project management plan which can contribute to a strategy for implementing the [*proprietary*] "technology stack"'. The new plan added, in effect, about a year to the project timetable.

Other changes

9.37 There have been subsequent changes to the CMAL implementation timetable. Two major aspects, each of which has had to be taken into account in CMAL implementation planning, are these:

- A recommendation of the Wheen Review was that DIAC undertake a 'proof of concept' process to assess the capacity of various options to enhance name searching on PAL. The options were various upgrades to the *SSAName3* name matching software. This led to the MASC (MAL Augmentation Search Capability) project, then scheduled for October 2006, which upgraded DIAC's version of *SSAName3* from 1.7 to 2.6.[303] CMAL now also became dependent on this project's successful implementation.
- The original improved secure communications system between DIAC and security agencies was further developed in a separate project, the

[301] DIAC advice of 22 January 2009.

[302] DIAC, agenda item for the Border Systems Board (BSB) meeting of 13 July 2006. The BSB chose not to endorse the plan at that time but to allow more time for review. It appears that no formal endorsement was recorded (DIAC advice of 22 January 2009).

[303] DIAC, *MAL Review Implementation—Project Sponsor Report*, July 2008. The 'proof of concept' work was regarded in the *CMAL Project Management Plan* v.3.0 of 21 July 2006 (p. 13) as 'out of scope' for the CMAL project but, nevertheless funded by the CMAL project.

Security Referral Service (SRS), which has also been implemented concurrently with the later stages of CMAL implementation.[304]

9.38 There have been other, minor changes to the CMAL timetable. Each such change has been supported by a formal Project Change Request, with a detailed rationale, consideration of the options and formal approval.[305] It is evident that DIAC has deliberately taken an incremental approach in extending CMAL processing and sought to learn from each stage.

Actual implementation

9.39 The CMAL application was first implemented with the third SfP release on the weekend of 13–14 October 2007. Business use of CMAL as a replacement for the previous visaload MAL check process began on 24 October 2007.[306] In effect, from this point CMAL took over the secondary check of clients who had already been granted a visa through one of the department's other visa processing systems (ICSE, IRIS, and ETAS). A backlog developed but this was controlled and eliminated by early April 2008.

9.40 Subsequently, CMAL has been extended to process Electronic Travel Authorities in the ETAS system (progressively from April to June 2008) and, concurrently, was deployed for use by overseas posts using the IRIS system from May 2008. CMAL for ICSE commenced in November 2008.

9.41 Ultimately, CMAL coverage for all DIAC's major visa processing systems was implemented in late 2008, rather than September 2006, as first envisaged.[307] Moreover, current scheduling shows further essential steps timed for future releases of SfP. For example, the HMAL database remains the primary MAL database and all maintenance of MAL data is performed on it. This is regularly copied into the CMAL database to keep it current. Maintenance of MAL records is scheduled to move from HMAL to CMAL in 2009, as preliminary step to ultimate decommissioning of Heritage MAL. That decommissioning, which will realise savings in processing costs, will not occur

[304] DIAC, MAL Review Implementation—Project Sponsor Report, July 2008.

[305] DIAC, email advice including copies of project change requests, 3 July 2008.

[306] DIAC, Quarterly Report—Movement Alert List—January–March 2008.

[307] DIAC has prepared briefs on progress with CMAL recently still in terms of four phases. However, the content of several of the phases has been restructured and is not the same as that set out in 2005. This makes it difficult to assess progress against the original plan.

before SfP release 10 or later. Therefore, full realisation of the benefits is not expected until 2010.[308]

Managing the processing backlogs

9.42 The new CMAL system was less efficient than expected and the throughput described as 'poor'. The backlog of unresolved possible matches peaked at 85 000 in early 2008. DIAC explained that the problems had been addressed by 'deploying technical fixes on a weekly basis' and increasing the number of staff available to resolve possible matches.[309]

9.43 Delays in clearing matches at visaload can easily affect client service at airports as the cases identified already have visas and may be travelling. That report also noted an adverse effect on client service:

> There remains a significant client service impact on outwards referrals at airports. [A] work around, although effective enough for the time being, has led to impacts to client service standards with some noted client delays.

9.44 The report did not quantify the client delays. However, it did provide a frank account of the degree of achievement of business objectives (such as could then be observed).

9.45 DIAC cleared the processing backlog by early April 2008 both by technical fixes and applying additional staff to clearing the backlog. The extension of CMAL to other systems proceeded.

CMAL is within budget

9.46 The then government agreed to the CMAL project and allocated the resources sought by DIAC for CMAL in the context of the 2005–06 Budget (see Table 9.1). Prima facie, CMAL is within budget as at January 2009 (Table 9.2). Use of the resources allocated has been below the allocation in the first year of the project, in particular due to the delays experienced by the project. Funding lapses on 30 June 2009, with the expectation that there would be a review in the context of the 2008–09 Budget.

[308] DIAC, SFP031-D, Central Movement Alert List (CMAL) Project Implementation Plan, SFP8, 16 October 2008.

[309] DIAC, SfP Benefits Realisation Report. This was prepared for DIAC's Systems Committee meeting of 17 January 2008. That Committee requires a report on the benefits realised through each release, three months after the release.

Table 9.1

CMAL resources allocated ($m)

	2005–06	2006–07	2007–08	2008–09	Total
Operating expenses	8.1	8.6	9.5	10.1	36.5
Capital	5.5	5.0	2.0	2.0	19.5

Source: DIAC, Initial Budget Allocation.

Table 9.2

CMAL resources used ($m)

	2005–06	2006–07	2007–08	2008–09	Total
Operating expenses	1.5	7.8	12.2	4.6*	26.1*
Capital	1.6	5.6	3.5	2.0	12.7

* YTD 21 January 2009.

Source: DIAC advice.

9.47 It is likely that the delays to the project have helped keep resource usage below budget. However, a further difficulty in assessing the financial management of the project is that DIAC was funded to implement the full suite of Wheen Review recommendations. As observed above, a substantial number of items that had been funded as part of the overall project were placed outside the scope of the core CMAL redevelopment project whereas the figures in Table 9.2 reflect the costs of the core project.

(d) Arrangements for review of the project

9.48 When seeking funding from government, DIAC proposed to review the project before 2008. The business case put to the then Department of Finance and Administration as part of the process of agreeing costs for the CMAL project included the following commitment for review:

> The performance of the new alert processor and 24/7 MAL Centre will be reviewed in 2008–09, to report back to Cabinet in the 2009–10 Budget process.

9.49 DIAC undertook reviews of certain stages of CMAL implementation. In particular, it had held meetings of the areas of the department most affected by the changes brought about by the initial CMAL implementation in October 2007. This was written up in a way that described those aspects that had worked well, those that had not worked and actions that were to follow.[310] However, these are operational-level activities of a different character to an overall, strategic review of the CMAL project against government-endorsed objectives.

9.50 Responsibility for a review plan was assigned to the 'Border Security Steering Committee'. However, the ANAO is unaware of any review so far that will address this requirement. DIAC advises that 'it will be appropriate to review the outcomes of the CMAL project at the completion of the [new policy proposal], so reporting should occur in 2009–10.'

Conclusion—the core project has been implemented

9.51 DIAC has successfully introduced the CMAL system, which now operates in all visa processing systems. DIAC has pursued CMAL implementation as its most important priority in MAL operations, following the actual MAL-checking role itself. It has fulfilled the relevant project objectives set out in the CMAL Baseline Project Management Plan (see para. 9.9). Most important, the CMAL implementation has addressed two major risks by using DIAC's stronger name-matching software in all MAL-matching and having possible matches decided by experts in the BOC (see para. 9.2).

9.52 CMAL implementation has taken two years longer than originally envisaged. During the project, DIAC's major Systems-for-People project introduced a new and different IT environment in which to progress, and this alone set the CMAL schedule back by about a year. However, despite the contingencies faced by the project over this time, DIAC has successfully managed its way through these and delivered its core undertakings.

9.53 Certain major tasks remain, such as decommissioning the old version of MAL, HMAL, and switching over wholly to the new system. Full realisation of benefits from the IT project will only be achieved after these changes have been implemented. Moreover, the original project encompassed measures agreed by the Government beyond the core IT redevelopment of MAL and centralising of MAL operations and which have not yet been implemented. These included the development of a reporting strategy and quality assurance process.

[310] DIAC, email advice of 12 May 2008.

9.54 DIAC has not pursued its original proposals for measuring and reporting the performance of this project, though it did report progress of the core project through the CIU while required to do so. However, arrangements should be in place to give confidence that the decisions of government are effectively implemented; and when major changes are necessary, that the stakeholders are appropriately informed.

9.55 DIAC has advised that it intends to report to government, through the portfolio minister, once the CMAL NPP project wraps up at the end of 2008–09. It has undertaken to present a complete overview of the project in early 2009–10 which will include reporting against its original project objectives, as agreed by government in 2005. This includes each item specifically identified in the approved proposal.

Ian McPhee

Auditor-General

Canberra ACT

21 May 2009

Appendices

Appendix 1: DIAC's reasons for entering a record on the Person Alert List

Alert Reason	Who should be listed
National Security	Any person known to be or suspected of posing a direct or indirect threat to Australian national security.
War Crimes or Human Rights Abuses	Persons who are known or suspected to have committed war crimes or other significant human rights abuses.
Controversial Visitors/Weapons of Mass Destruction	Persons to whom grant of a visa, ETA or Australian citizenship may cause national controversy.
Serious or High Profile Crime	Persons suspected or convicted of committing crimes of serious concern to the Australian community.
Organised Immigration Malpractice	Persons engaged in the organisation of known or suspected immigration fraud rackets such as people smuggling, document fraud, illegal prostitution, other illegal employment and bogus marriages.
Travel Sanctions	Persons subject to UN Security Council resolutions imposing travel sanctions or bilateral sanctions or travel sanctions as imposed by the Foreign Minister.
Serious Criminal (poor bio data)	Persons who would otherwise be listed under 'Serious or high profile crime' but do not meet the minimum data standard (for example, no date-of-birth).
Health Concerns	Persons not meeting relevant health criteria for visa grant, or persons whose applications have been refused on health grounds, or applicants deferred for further testing and/or treatment in relation to tuberculosis or any disease or condition which represents a public health risk.
Child Custody Concerns	Persons under 18 years, where grant of visa to such persons may prejudice a contact, residence or child maintenance order or any other formal maintenance obligation to that person, or persons under 18 years for whom a credible representative (for example, legal, religious, family) claims to have a contact, residence or child maintenance order or access rights or any other formal maintenance obligation and objects to the under 18 year old being granted a visa on the basis that the representative's contact, residence or child maintenance rights may be prejudiced. The above claim must be clearly stated orally or in writing.

Alert Reason	Who should be listed
Other Criminals	Persons known or suspected of being involved in crimes not serious enough to be listed under ‘Serious or high profile crime’ including (but not limited to), theft, burglary, minor assault, or fraud.
Overstayers	Persons who are subject to [Migration Act] public interest criterion 4014.
Breach of Visa conditions	Persons who may be subject to public interest criterion 4013 for cancellation of a temporary visa under s116 of the Migration Act, for example, working without authority, failure to comply with a condition specified in public interest criterion 4013 (Satisfactory Attendance and Performance by Students).
Debts to the Commonwealth	Persons with a debt to the Commonwealth that may be taken into account for a decision regarding any subsequent visa. The debt may have arisen from detention or removal costs, litigation costs, social security debts, taxation debts; or any other source of debt to the Commonwealth.
Immigration Malpractice	Persons whose visa has been cancelled and are subject to an exclusion period or presented false documents, or refused entry on false documents.
Refused/Bypassed Immigration Clearance	Bypassed immigration clearance processes on entry (for example, stowaways or boat arrivals); or refused immigration clearance whether air or boat arrival.
Suspect Genuineness	Persons suspected, based on reasonable belief and substantial evidence, of misleading or likely to mislead a decision-maker about any matter that would have significant bearing on the outcome of the person’s application, or incentive to travel, family travel and application history, applying outside country of normal residence.
Surrender Australian Travel Document	Persons who are travelling to Australia on Australian travel documents that are damaged or in poor condition. Under the *Australian Passport Act 2005* any Australian travel document that is considered “damaged” is considered invalid and therefore is required to be surrendered.
Illegal Fishers	Persons detected fishing illegally in Australian waters

Source: DIAC, PAM3 manual.

Appendix 2: Statistical tables

Table A 1

Numbers of PAL records, by Alert Reason, 1997–2008

Alert Reason (and Risk)	19 Oct. 1997	30 June 2000	30 June 2002	30 June 2003	30 June 2004	18 July 2008
National Security (high)	4 357	31 272	43 645	51 390	92 369	379 804
Terrorism (high) [No longer used]	357	126	129	149	247	NA
War Crimes/Human Rights abuses (high)	805	1 475	6 569	6 915	7 212	7 438
Controversial Visitors (high)	340	1 361	1 725	1 953	2 000	1 497
Serious / High Profile Crime (high)	15 777	23 180	27 857	30 593	34 056	64 591
Organised Immigration Malpractice (high)	400	3 988	5 806	7 235	7 974	12 120
Travel Sanctions (high)	NA	NA	NA	NA	NA	4 195
Serious Crime (Poor Bio data) (high)	NA	270	227	255	367	724
Health Concerns (med.)	1 246	7 790	12 700	18 607	25 928	57 954
Child Custody Concerns (med.)	234	665	827	977	1 210	1 967
Other Criminals (med.)	3 163	21 124	26 874	30 849	33 396	44 669
Overstayers (low)	19 451	22 026	29 100	31 064	33 301	28 860
Breach of Visa Conditions (low)	141	7 495	15 895	17 785	19 458	15 258
Debts to the Commonwealth (low)	62	11 082	12 421	16 505	30 559	38 223
Immigration Malpractice (low)	2 369	5 170	5 776	4 848	5 652	13 960
Refused Immigration Clearance (low)	438	2 903	3 697	2 062	2 280	4 632
Suspect Genuineness (low)	993	5 130	7 404	11 559	13 199	11 414
Surrender Australian Travel Document	NA	NA	NA	NA	NA	11
Illegal Fishers (low)	NA	NA	NA	NA	NA	54
Total	**50 133**	**145 057**	**200 652**	**232 746**	**309 208**	**687 371**

Sources: 19 October 1997: Sadleir Review. 30 June 2000, 30 June 2002, 30 June 2003 and 30 June 2004: Wheen Review. 18 July 2008: ANAO testing of MAL database.

Table A 2

National security PAL records: value analysis of common fields

Column Name	Percentage of values occurring only once		Percentage blank		Percentage marked as ‘unknown’		Percentage of values occurring more than once	
	March 06	*July 08*	*March 06*	*July 08*	*March 06*	*July 08*	*March 06*	*July 08*
Person Number	100.00	100.00						
Family Name	42.10	20.51				+	57.90	79.49
Given Name	47.48	33.85		0.30^			52.52	65.85
Date of Birth	8.16	0.43		0.04			91.84	99.53
Country of Birth	0.08		83.54	84.53		8.09	16.38	7.38
Citizenship	4.21		0.10	1.64		28.91	95.69	69.45
Sex			1.69	1.00		1.49	98.31	97.51
Entered Date	96.00	0.10					4.00	99.90
File Number	0.08	0.03	98.82	99.34			1.10	0.63
Alias			84.65	90.93			15.35	9.07
Informer	0.01		98.88	99.39			1.11	0.61
Primary Reason							100.00	100.00
Secondary Reason	0.02		98.37	98.85			1.61	1.15
External Agency ID		90.94	100.00	0.08				8.98
Narrative	*	11.72	*	77.34	*		*	10.94

Source: March 2006 data—derived from DIAC ‘data mining’ analysis; July 2008—ANAO testing.

Note that the data for these records is almost wholly sourced from security agencies. The above table is a summary of the PAL fields most commonly used. ‘Values occurring once’ indicates that that value does not recur in that field throughout the dataset. ‘Blank’ indicates the proportion of records which have no characters in that field. ‘Marked as Unknown’ shows the proportion of records which contain ‘Unknown’ for that field.

+ Contains a small number of entries undetected by rounding.
^ Null entries: records which contain invalid characters such as punctuation marks.
* No data available.

What the July 2008 value analysis reveals: *National Security* records

(1) There are 379 804 records listed with a primary Alert Reason of *National Security*.

(2) All PAL records have an individual *Person Number*, which DIAC uses as an individual identifier. There are no duplicates, invalid numbers or numbers missing.

(3) Only one record has 'Unknown' as *Family Name*, and no null entries (comprising invalid characters) exist. Some 14 records contain only one character for *Family Name*.

(4) Some 1140 records have a null entry for the *Given Name* field, being a dash. However, having only one name occurs in some countries (such as Indonesia). Some 17.45 per cent of these have various combinations of *Citizenship* and *Country of Birth* as Indonesian.

(5) Some 18 records have a unique entry for *Country of Birth*. That is, there are 18 persons listed who are each the only person recorded on PAL with that *Country of Birth*. There are 13 records with a unique entry for *Citizenship*. The ANAO confirms that all country codes recorded in these fields are legitimate.

(6) For the *Sex* field, 9456 records are either blank or marked as 'Unknown sex'.

(7) The *Entered Date* field holds the creation date of the record. Each record contains a valid date between 22 August 1983 (the first recorded PAL entry) and 18 July 2008.

(8) The *File Number* is used to record the physical or electronic reference to further information regarding the record. Two records have a null entry for *File Number*, created in 2002 and 2003.

(9) The *Alias* field indicates there is a known alternate identity the person has used or is likely to use, which relates to a primary PAL record. A substantial majority of records (90.93 per cent) do not have an *Alias*.

(10) Every record has a *Primary Alert Reason,* used to identify the reason for the alert creation. Some 4354 records contain at least one *Secondary Alert Reason.*

(11) The field *External Agency ID* is the reference number used by the external owner of primary reason of *National Security*, where the record has originated at the request of that agency. There are 286 records with blank *External Agency ID*, 54.90 per cent of which were created since 1 January 2005.

(12) The *Narrative* field is a free-text box used to explain the reason for the record, to assist DIAC decision-makers. Some 41 553 records have identical narrative, and 77.34 per cent of all *National Security* records have an empty *Narrative* field.

Table A 3

PAL records: Value Analysis of common Non-National Security fields

Column Name	Percentage of unique occurrences	Percentage blank	Percentage marked as 'unknown'	Percentage of multiple occurrences
	July 08	*July 08*	*July 08*	*July 08*
Person Number	100.00			
Family Name	24.09			75.91
Given Name	37.83	2.01^		60.16
Date of Birth	0.76	2.13		97.11
Country of Birth		2.11	18.40	79.49
Citizenship		3.81	9.09	87.10
Sex		1.70	1.21	97.09
Entered Date	0.07			99.93
File Number	24.23	48.97		26.80
Alias		73.37		26.63
Informer		69.89		30.11
Primary Reason				100.00
Secondary Reason	0.02	82.25		17.73
External Agency ID	0.11	99.42		0.47
Narrative	61.34	0.05		38.61

Source: Results of ANAO testing of MAL database dated 18 July 2008 comparing to DIAC testing of database dated March 2006.

Note: The above table is a summary of the PAL fields most commonly used. 'Unique occurrences' indicates PAL records which are unique to the data set. 'Blank' indicates the number of records which have no characters in that field. 'Marked as "unknown"' shows records which contain 'Unknown' for that field. 'Multiple occurrences' indicates the number of entries repeated in the data set.

+ Contains a small number of entries undetected by rounding.
^ Null entries: records which contain invalid characters such as punctuation marks.
* No data available.

What the July 2008 value analysis reveals: Non-*National Security* records

(1) There are 307 567 records listed in PAL against with a primary Alert Reason other than *National Security*.

(2) All PAL records have an individual *Person Number*, which DIAC uses as an individual identifier. That is, there are no duplicates, invalid numbers or numbers missing.

(3) There are no defective entries for the *Family Name* field. However, 52 records contain only one character for *Family Name* (Some or all of these may be valid).

(4) Some 6176 records have a null entry for the *Given Name* field, being a dash. However, having only one name occurs in some countries (such as Indonesia). Some 59.01 per cent of these have various combinations of *Citizenship* and *Country of Birth* as Indonesian.

(5) Some 15 records have a unique entry for *Country of Birth*. That is, there are 15 persons listed who are each the only person recorded on PAL with that *Country of Birth*. There are 18 records with a unique entry for *Citizenship*. The ANAO confirms that all country codes recorded in these fields are legitimate, except one, now obsolete.

(6) For the *Sex* field, 8945 records are either blank or marked as ‘Unknown sex’.

(7) Each record contains the date that record was created under *Entered Date*.

(8) Seven records have a null entry for *File Number*. Most were created before 2003; however, two were created in 2007.

(9) Nearly three-quarters of these records (73.37 per cent) do not have an *Alias*.

(10) Every PAL record has a valid *Primary Alert Reason*. Some 54 527 contain at least one *Secondary Alert Reason*.

(11) The field *External Agency ID* is the reference number used by an external agency where the record has originated at the request of that agency. There are 1790 records which contain this number.

(12) Some 118 760 records have an identical *Narrative*. This is due to the use of ‘Refer to Character section’ and 156 records have nothing in the narrative field.

Table A 4

Data deficient records in PAL (27 November 2003)

Alert Reason	Number of records with this primary Alert Reason	Number of these records that are data deficient	Percentage of these records that are data deficient
National Security	68 899	8 891	12.90
Terrorism	238	52	21.85
War crimes / Human Rights Abuses	7 118	3 791	53.26
Controversial Visitors	1 949	555	28.48
Serious or High Profile Crime	31 953	1 757	5.50
Organised Immigration Malpractice	7 552	258	3.42
Travel Sanctions	0	0	0.00
Serious Criminal (Poor bio data)	282	221	78.37
Health Concerns	21 915	8 447	38.54
Child Custody Concerns	1 059	40	3.78
Other Criminals	32 338	703	2.17
Overstayers	32 921	1	0.00
Breach of Visa Conditions	19 107	0	0.00
Debts to the Commonwealth	19 410	0	0.00
Immigration Malpractice	5 279	7	0.13
Refused Immigration Clearance	2 140	0	0.00
Suspect Genuineness	12 913	22	0.17
Surrender Australian Travel Document	0	0	0.00
Illegal Fishers	0	0	0.00
Total	265 073	24 745	9.34
Without National Security cases	*196 174*	*15 854*	*8.08*

Source: ANAO re-calculation of Table 3 in the report of the Wheen Review without the redundant test.

Note: 'Data deficiency' is the term used by the Wheen Review to characterise incomplete MAL records.

Table A 5

Data deficient records in PAL (18 July 2008)

Alert Reason	No. of records with this primary reason	No. of these records that are data deficient	Percent-age that are data deficient	Excluding *National Security* records, Percentage of all data deficient records that are in this reason
National Security	379 804	105 464	27.77	–
Terrorism [*No longer used*]	0	0	0.00	0.00
War Crimes / Human Rights Abuses	7 438	3 650	49.07	11.68
Controversial Visitors	1 497	277	18.50	0.89
Serious or High Profile Crime	64 591	2 011	3.11	6.43
Organised Immigration Malpractice	12 120	313	2.58	1.00
Travel Sanctions	4 195	1 385	33.02	4.43
Serious Criminal (Poor bio data)	724	535	73.90	1.71
Health Concerns	57 954	22 150	38.22	70.88
Child Custody Concerns	1 967	66	3.36	0.21
Other Criminals	44 669	863	1.93	2.76
Overstayers	28 860	0	0.00	0.00
Breach of Visa Conditions	15 258	0	0.00	0.00
Debts to the Commonwealth	38 223	2	0.01	0.01
Immigration Malpractice	13 960	0	0.00	0.00
Refused Immigration Clearance	4 632	0	0.00	0.00
Suspect genuineness	11 414	0	0.00	0.00
Surrender Australian Travel Document	11	0	0.00	0.00
Illegal Fishers	54	0	0.00	0.00
TOTAL	**687 371**	**136 716**	**19.89**	
Without National Security	*307 567*	*31 252*	*10.16*	

Source: ANAO analysis of dataset provided by DIAC.

Table A 6

Records with a review period inconsistent with DIAC policy

NB: DIAC policy is taken as that set out in the department's PAM3 manual.

Alert Reason	Review period specified in PAM3 for this Alert Reason	No. of records where review period is ...		
		less than PAM3	consistent with PAM3	exceeds PAM3
National Security	(i) Age 80	3 159	371 520	4 991
	(ii) Where DOB unknown, 60 years from creation	59	69	6
War Crimes	10 years from creation	5 208	850	1 380
Controversial Visitors	10 years from creation	162	405	930
Serious Crime	Age 100	11 300	42 685	10 606
Organised Immigration Malpractice	(i) People smuggling—Age 100	0	6	0
	(ii) Otherwise—review 10 years from creation	1 239	4 732	6 143
Travel Sanctions	Review in 5 years from creation	176	1 531	2 488
Serious Criminal (Poor Bio data)	Review in 2 years from creation	1	4	719
Health Concerns	Age 120 or (formerly) 100	865	56 463	626
Child Custody Concerns	Age 18	86	1 543	338
Other Criminals	(i) Age 100 (or Australian Citizenship)	8 518	31 103	5 010
	(ii) 10 years if breach of *Foreign Acquisitions and Takeovers Act 1976*	1	0	37
Overstayers	3 years from creation	166	15 809	12 885
Breach of Visa Conditions	3 years from creation	165	11 562	3 531
Debts to the Commonwealth	<$1000 – 10 years from creation >$1000 – Age 100	*Unknown (cannot be calculated on available data)*		
Immigration Malpractice	3 years from creation	95	10 518	3 347
Refused Immigration Clearance	3 years from creation	72	3 373	1 187
Suspect Genuineness	3 years from creation	316	8 358	2 740
Surrender Australian Travel Document	1 year from creation	1	1	9
Illegal Fishers	3 years from creation	33	4	17
	Total	**87 826**	**504 332**	**56 990**

Source: Results of ANAO testing of MAL database dated 18 July 2008. Note that 'Age' means the age of the person, not the age of the record.

Appendix 3: DIAC's primary visa and citizenship processing systems

IRIS—IRIS operates at all DIAC overseas posts and is also used within Australia to process certain offshore visas. Details of visas granted are transmitted overnight from the posts to Australia. Before the introduction of CMAL, IRIS held a local copy of PAL data and was sent updates of the PAL data twice a day. This local copy of MAL was used to check the visa applicants for PAL matches. IRIS performed PAL checks multiple times (including when the applicant's details are recorded and then again just prior to the granting of the visa). If any of these PAL checks resulted in possible matches then the staff at the post would examine them and determine if there was a definite match and whether it was relevant. IRIS did not check DAL.

ICSE—ICSE is DIAC's generic client system used to maintain information on client requests for citizenship and onshore visa grants. ICSE provides on-line processing and decision recording and operates at all on-shore DIAC offices. ICSE first performs a MAL check when the applicant's details are recorded and then again just prior to the granting of the visa if more than 24 hours have passed since the last MAL check. Before CMAL, if a MAL check resulted in possible matches then the DIAC officer processing the visa would examine those matches to determine if there were any definite matches.

ETAS and APP (Advance Passenger Processing)—Electronic Travel Authority (ETA) visas are available to short stay tourist and business visitors from selected countries. The ETA system, ETAS, is designed so travel agents or airline reservations personnel can apply for an ETA for a client at the time of booking a flight to Australia. After checking MAL, a response, of either granting the ETA or referring the applicant to the local DIAC post, is returned to the agent within seconds. A person can also apply for an ETA over the Internet.

The Advance Passenger Processing (APP) system enables airline departure control staff to verify that all passengers destined for Australia have authority to travel to Australia. Instead of checking for the presence of a visa label in the passenger's passport, the authority for a passenger to travel is available electronically. The APP system improves the processing of passengers as they arrive in Australia as advance notice of the arrival of each passenger is provided to DIAC and Customs and Border Protection.

The ETAS and APP systems are maintained and hosted by a third party contractor. Before CMAL, a copy of MAL data was held locally by the contractor to enable the checking of ETA applicants by ETAS and the travel documents of passengers by APP. Updates to the MAL data were delivered to the contractor at least hourly. If the ETAS MAL check resulted in one or more possible matches then the travel agent or airline was informed that the applicant will need to apply for a visa at a DIAC overseas post. The APP system checks the passenger's travel document against DAL to confirm that it has not been listed as lost or stolen.

The Visaload process

The Visaload component of DIAC’s Visa Manager System loads visa records created by other systems (mainly ETAS, IRIS, and ICSE) onto the TRIPS Visa database. Visa data is then made available to other systems, both internal and external to DIAC.

The Visaload uses a MAL application program interface (called ‘SNAPIS’) to access MAL. The MAL check is both a person check (PAL) and a document check (DAL). Any possible matches that arise from the Visaload MAL check are reviewed by the EOC.

Appendix 4: Reports on MAL performance proposed by Wheen

General

- Numbers of records x alert codes (monthly for Section/Branch heads—quarterly for senior managers)
- Nos of records on DAL
- Nos of notifications received each day at Visaload (daily for EOC, MABSS)
- Nos of notifications not 'cleared' at Visaload within 24 hours of receipt (ditto)
- Nos of updates not entered within 24 hours of receipt (ditto)
- Nos of notifications cleared (at Visaload) by individual operators—(as necessary—supervisors)
- Nos of notifications in IRIS search (each day) x Post (monthly Section Heads)
- Nos of deferrals in ETAS search (each day) x travel agent (monthly Section Heads)
- Nos of notifications in ICSE x office (monthly Section Heads)
- Nos of visa grants (Visaload) and nos of visas granted in each of IRIS, ETAS and ICSE (monthly Section heads)
- Nos of PAL notifications by risk category, including numbers which contain more than one risk category (monthly Section and Branch heads – quarterly Senior managers)
- Nos of visa applications which result in an [*National Security*] notification and the numbers of [*National Security*] notifications (monthly Section and Branch heads—quarterly senior managers)
- Nos of visas which result in a true match x alert code
- Nos of visas which result in a true match x alert code x subsequent action taken
- Nos of each of PAL (x alert codes) and of DAL records—created/updated/deleted (all separately) (monthly Section and Branch Heads)

Data Quality

- Against criteria to be established, report on completeness of records x alert codes x PIDs—to enable follow up on those records which are data deficient (daily for [certain DIAC sections])
- Against criteria to be established, report on the completeness of records x alert codes (quarterly—all managers)
- New entries/ updates/deletes x RIF (ditto)
- New entries and entries/updates/deletes x 774s (ditto)
- Monitoring a range of trends/patterns

Training Activities

- Nos of staff trained x location x period (quarterly—Section/Branch heads)
- How do we get a quality measure? One measure is client evaluation following training but other could include appropriate assessment of trainees

Quality Assurance Reporting

- Range of sampling measures re data quality, new entries, updates
- Monitor trends in changes in profile of records

Information for Business Managers on Systems Operation

- Report on any mainframe outages (scheduled and non scheduled) impacting MAL system usage
- Same as above for citizenship processing and for Visaload
- Audit functionality to identify who changes IRIS thresholds

Information for Systems Managers on Business operations

- Timely advance warnings of bulk loads.

Series Titles

ANAO Audit Report No.1 2008–09
Employment and Management of Locally Engaged Staff
Department of Foreign Affairs and Trade

ANAO Audit Report No.2 2008–09
Tourism Australia
Tourism Australia

ANAO Audit Report No.3 2008–09
Establishment and Management of the Communications Fund
Department of Broadband, Communications and the Digital Economy
Department of Finance and Deregulation

ANAO Audit Report No.4 2008–09
The Business Partnership Agreement between the Department of Education, Employment and Workplace Relations (DEEWR) and Centrelink
Department of Education, Employment and Workplace Relations
Centrelink

ANAO Audit Report No.5 2008–09
The Senate Order for Departmental and Agency Contracts (Calendar Year 2007 Compliance)

ANAO Audit Report No.6 2008–09
Illegal, Unreported and Unregulated Fishing in the Southern Ocean
Australian Customs Service

ANAO Audit Report No.7 2008–09
Centrelink's Tip-off System
Centrelink

ANAO Audit Report No.8 2008–09
National Marine Unit
Australian Customs Service

ANAO Report No.9 2008–09
Defence Materiel Organisation–Major Projects Report 2007–08

ANAO Audit Report No.10 2008–09
Administration of the Textile, Clothing and Footwear Post–2005 (SIP) Scheme
Department of Innovation, Industry, Science and Research

ANAO Audit Report No.11 2008–09
Disability Employment Services
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.12 2008–09
Active After-school Communities Program
Australian Sports Commission

ANAO Audit Report No.13 2008–09
Government Agencies' Management of their Websites
Australian Bureau of Statistics
Department of Agriculture, Fisheries and Forestry
Department of Foreign Affairs and Trade

ANAO Audit Report No.14 2008–09
Audits of Financial Statement of Australian Government Agencies for the Period Ending June 2008

ANAO Audit Report No.15 2008–09
The Australian Institute of Marine Science's Management of its Co-investment Research Program
Australian Institute of Marine Science

ANAO Audit Report No.16 2008–09
The Australian Taxation Office's Administration of Business Continuity Management
Australian Taxation Office

ANAO Audit Report No.17 2008–09
The Administration of Job Network Outcome Payments
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.18 2008–09
The Administration of Grants under the Australian Political Parties for Democracy Program
Department of Finance and Deregulation

ANAO Audit Report No.19 2008–09
CMAX Communications Contract for the 2020 summit
Department of the Prime Minister and Cabinet

ANAO Audit Report No.20 2008–09
Approval of Funding for Public Works

ANAO Audit Report No.21 2008–09
The Approval of Small and Medium Sized Business System Projects
Department of Education, Employment and Workplace Relations
Department of Health and Ageing
Department of Veterans' Affairs

ANAO Audit Report No.22 2008–09
Centrelink's Complaints Handling System
Centrelink

ANAO Audit Report No.23 2008–09
Management of the Collins-class Operations Sustainment
Department of Defence

ANAO Audit Report No.24 2008–09
The Administration of Contracting Arrangements in relation to Government Advertising to November 2007
Department of the Prime Minister and Cabinet
Department of Finance and Deregulation
Department of Education, Employment and Workplace Relations
Department of Health and Ageing
Attorney-General's Department

ANAO Audit Report No.25 2008–09
Green Office Procurement and Sustainable Office Management

ANAO Audit Report No.26 2008–09
Rural and Remote Health Workforce Capacity – the contribution made by programs administered by the Department of Health and Ageing
Department of Health and Ageing

ANAO Audit Report No.27 2008–09
Management of the M113 Armoured Personnel Upgrade Project
Department of Defence

ANAO Audit Report No.28 2008–09
Quality and Integrity of the Department of Veterans' Affairs Income Support Records
Department of Veterans' Affairs

ANAO Audit Report No.29 2008–09
Delivery of Projects on the AusLink National Network
Department of Infrastructure, Transport, Regional Development and Local Government

ANAO Audit Report No.30 2008–09
Management of the Australian Government's Action Plan to Eradicate Trafficking in Persons
Attorney-General's Department
Department of Immigration and Citizenship
Australian Federal Police
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.31 2008–09
Army Reserve Forces
Department of Defence

ANAO Audit Report No.32 2008–09
Management of the Tendering Process for the Construction of the Joint Operation Headquarters
Department of Defence

ANAO Audit Report No.33 2008–09
Administration of the Petroleum Resource Rent Tax
Australian Taxation Office

ANAO Audit Report No.34 2008–09
The Australian Taxation Office's Management of Serious Non-Compliance

Current Better Practice Guides

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

Developing and Managing Internal Budgets	June 2008
Agency Management of Parliamentary Workflow	May 2008
Public Sector Internal Audit	
An Investment in Assurance and Business Improvement	Sep 2007
Fairness and Transparency in Purchasing Decisions	
Probity in Australian Government Procurement	Aug 2007
Administering Regulation	Mar 2007
Developing and Managing Contracts	
Getting the Right Outcome, Paying the Right Price	Feb 2007
Implementation of Programme and Policy Initiatives:	
Making implementation matter	Oct 2006
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
Building Capability—A framework for managing learning and development in the APS	Apr 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