The Auditor-General
Audit Report No.20 2013–14
Performance Audit

Management of the Central Movement Alert List: Follow-on Audit

Department of Immigration and Border Protection

Australian National Audit Office

ISSN 1036–7632
ISBN 0 642 81428 7 (Print)
ISBN 0 642 81429 5 (Online)

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

Or via email:
publications@anao.gov.au

Australian National
Audit Office

Canberra ACT
20 February 2014

Dear Mr President
Dear Madam Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Department of Immigration and Border Protection titled *Management of the Central Movement Alert List: Follow-on Audit.* The audit was conducted 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 to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website—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, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

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

Phone: **(02) 6203 7505**
Fax: **(02) 6203 7519**
Email: **publications@anao.gov.au**

ANAO audit reports and information about the ANAO are available on our website:

http://www.anao.gov.au

Audit Team
Robina Jaffray
Benjamin Siddans
William Na/Jerry Liao
Tom Clarke

Contents

Tables

Figures

Abbreviations and Glossary

AFP	Australian Federal Police
APP	Advance Passenger Processing, an electronic system that collects information on all passengers and crew, including all transit passengers, travelling to Australia for cross-checking against Australia's immigration databases.
ARC	Alert Reason Code, which is used to classify alerts within the Person Alert List database. Each ARC is categorised according to risk (high or medium or low).
ASIO	The Australian Security Intelligence Organisation.
BOC	Border Operations Centre, comprising the Central Movement Alert List, Entry Operations Centre and Travel and Immigration Processing System Helpdesk functions.
BOSS	Border Operations Support Section, a section within the Borders Operations Branch.
CMAL	Central Movement Alert List, the system interface with the Movement Alert List database used to identify travellers who may present immigration or national security risks to Australia.
Customs	Australian Customs and Border Protection Service.
DAL	Document Alert List, containing records of lost, stolen or fraudulent travel documents.
Decision maker	Any departmental officer who is lawfully delegated under the relevant Act to make decisions on granting, cancelling or refusing visas, approving or refusing citizenship; or making immigration clearance decisions.
DFAT	Department of Foreign Affairs and Trade

DIBP	Department of Immigration and Border Protection, formerly the Department of Immigration and Citizenship
ICSE	Integrated Client Service Environment
ISR	Identity Services Repository, DIBP's corporate store of identities (or client records) and documents.
IRIS	Immigration Records Information System
JCPAA	Joint Committee of Public Accounts and Audit
MAL	Movement Alert List
MAL check	An operation performed, at a point in time, to confirm whether active PAL or DAL records exist in relation to an individual or a travel document.
MAL status	The MAL status indicates a departmental client record either matches against a PAL or DAL record (red), or does not match a PAL or DAL record (green), or may potentially match a PAL record (amber).
MDS	Minimum Data Standards
Migration Act	*Migration Act 1958*
Override code	The act of a decision maker to temporarily suspend the effect of an amber or red MAL status. The override code allows the decision maker to grant a visa or citizenship.
PACE	Passenger Analysis, Clearance and Evaluation system
PAL	Person Alert List
PAL alert (PAL record)	An entry on PAL consisting of biographical and travel document data and a narrative description of the nature of the alert associated with that entry. One or more PAL records may exist for the same identity listed on PAL.

PAM3 Procedures Advice Manual

Potential match A match identified by the matching software is a potential match. Each potential match must be examined by a CMAL operations section match analyst for resolution.

RIF Remote Input Function, the interface used by visa processing officers, compliance staff and airport/seaport inspectors, ARC owners and other DIBP staff as required, to propose new PAL or DAL alerts or updates to existing alerts.

SmartGate An automated border processing system that enables eligible travellers arriving into Australia's international airports to self-process through passport control. It uses the data in ePassports and facial recognition technology to perform the customs and immigration checks that are usually conducted by an Australian Customs and Border Protection Service officer.

TRIPS Travel and Immigration Processing System

True match A true match occurs when either a BOC match analyst concludes biographical or travel document information contained in a client record corresponds to a PAL record or a DAL record matches a client travel document. A true match is either a PAL match or a DAL match and will create a MAL status of red.

Summary and Recommendations

Summary

Introduction

1. The Central Movement Alert List (CMAL) is an electronic watch list, containing information about individuals who pose either an immigration or national security concern to the Australian Government as well as information on lost, stolen or fraudulent travel documents. It is an integral part of Australia's layered approach to border security, identifying people of concern prior to their arrival at the border. CMAL is managed by the Department of Immigration and Border Protection (DIBP).[1]

2. Australia's universal visa system requires non-Australian citizens or permanent residents intending to enter or transit through Australia to obtain either a visa or an Electronic Travel Authority. All travellers entering Australia are therefore checked against CMAL, usually at several points along the travel pathway and generally at some distance from the physical border. CMAL information is also taken into account when DIBP assesses applications for Australian citizenship.

3. Passenger movements into and out of Australia are increasing annually: from approximately 17 million per annum in 2000–01 to almost 30 million in 2011–12. This number is expected to rise to 50 million per annum by 2020.[2] DIBP will need to have the capability and capacity to meet the challenges presented by these expected demands.

4. CMAL comprises two databases, the Person Alert List (PAL) and the Document Alert List (DAL). The PAL database stores the biographical details of identities of concern and DAL is a list of lost, fraudulent or stolen travel documents.[3] DIBP advised that, as at 30 November 2013 the CMAL database:

- contained 683 287 primary identities on PAL;
- contained 969 320 travel documents on DAL; and

[1] The Department of Immigration and Citizenship (DIAC) became the Department of Immigration and Border Protection following the machinery of government changes in September 2013.

[2] DIAC, *Annual Report 2011–12*, p. 145.

[3] DAL documents can be either Australian or foreign documents. DFAT is notified of travel documents of concern by international partners and these may be listed on DAL.

- generated 306 509 potential match cases per month on average, which resulted in 174 415 true matches between November 2012 and November 2013.

5. PAL records are categorised according to the reason for listing the identity—the alert reason code (ARC). There are 19 ARCs with each being categorised as high, medium or low risk. The national security ARC contains the largest single set of records and comprises approximately half the PAL database.

6. Using name matching software, the CMAL system queries its data holdings and identifies and presents potential or likely matches for Border Operations Centre (BOC) staff to assess. Potential match cases (amber status) are resolved by DIBP's BOC match case analysts to be either red or green.[4] When assessing visa or citizenship applications the DIBP decision maker must take this information into account before proceeding further.[5]

Key stakeholder agencies

7. In addition to DIBP, there are several Australian government agencies with an interest in CMAL. These include the:

- Australian Security Intelligence Organisation (ASIO);
- Australian Customs and Border Protection Service (Customs);
- Australian Federal Police (AFP); and
- Department of Foreign Affairs and Trade (DFAT).

These agencies either directly list alerts, contribute information for the listing of alerts or, in the case of Customs, manage incoming passenger movements on behalf of DIBP.

Developments in CMAL's strategic environment

8. DIBP's management of CMAL is undertaken within the context of the system's dual immigration and border security functions. Whole-of-government initiatives focused on the development of an integrated border

[4] A CMAL green status means there is no information in CMAL which decision makers need to take into account in making their decsion to grant a visa or citizenship.

[5] A CMAL red status will not necessarily mean that entry to Australia or Australian citizenship will be denied; it is one piece of information considered by DIBP's decision makers.

security alert strategy are currently under consideration. The multi-agency Border Management Group (BMG)[6], established in 2009 and chaired by Customs, is responsible for undertaking the detailed work required to implement, review and evaluate strategic border management planning activity, which may include CMAL. DIBP's strategic management of CMAL can be expected to take into acount any whole-of-government strategies for the protection of Australia's borders.

Previous reviews

9. CMAL was introduced progressively in 2008 and 2009, replacing the previous decentralised Movement Alert List (MAL) system as the operational database.[7] Successive reviews of MAL had judged it to be conceptually sound, but had also identified a number of operational and management deficiencies.[8] The Wheen review, undertaken in 2003, in particular found that:

- there was an increasing number and proportion of data deficient alerts, emphasising the need for effective quality assurance processes;
- effective reporting was needed to promote awareness of MAL's performance and to manage the business to achieve optimal outcomes;
- future management arrangements should include quality assurance processes to monitor and analyse trends and patterns of data, as well as feedback from users;
- MAL had become a system serving the whole of government and an inter-agency forum should be established to consider agencies' interests in the operations and future directions of CMAL;
- negotiation of a formal understanding with ASIO to establish the extent of DIBP's responsibility for the acceptance of and processing of national security alerts; and
- 'instructions' to be developed covering the limited circumstances in which it would be appropriate to record Australian citizens on MAL.

[6] The BMG has a membership of 12 border agencies, including DIBP.

[7] This report uses 'CMAL' to describe the current system and 'MAL' when talking about the database as it operated prior to the introduction of CMAL.

[8] Wheen D, *Report of the Review of the Purpose, Architecture and Operation of the Movement Alert List (MAL)*, 12 August 2004. Similar findings were highlighted in by Sadleir D, *Australia's Entry Control Arrangements: A Review*, January 1998 and Gerlach T, *A Technical/Operational Review*, April 2000.

10. The Wheen review also identifed the future need for MAL to have the capability to incorporate new technologies, such as biometrics as valuable additions in the identification of people of concern.

11. The ANAO undertook a performance audit of the management of the MAL in 2008–09.[9] This audit also confirmed that MAL was conceptually sound and that the Department had managed an extended period of growth in records. However, the lack of strategic or management planning for the database and the poor quality of the data contained within it, particularly its 'completeness, quality and currency', compromised the system's effectiveness. MAL quality assurance, and performance and management reporting arrangements were highlighted as requiring attention, as were the procedures governing the listing of Australian citizens on MAL. The ANAO made five recommendations (outlined in Appendix 2) to improve the administration of the MAL database.

12. Following the tabling of the audit report in May 2009, the Joint Committee of Public Accounts and Audit, (JCPAA), considered the report as part of its ongoing review of the Auditor-General's reports. The JCPAA recommended that the department report back within six months identifying 'instances where MAL had alerted its decision makers to information that has been the reason, or part of the reason, for decisions on visa and citizenship applications'. The department provided the JCPAA with information primarily relating to the 2009–10 financial year, that it considered demonstrated CMAL's contribution to Australia's border protection strategy at that particular point in time.[10] The Committee also proposed that the department implement the ANAO recommendations in relation to the recording of Australian citizens on the system.[11]

[9] ANAO, Audit Report No. 35, 2008–09, *Management of the Movement Alert List*, 9 May 2009.

[10] DIBP, Executive Minute to JCPAA,Review of Auditor-General's Reports tabled between February 2009 and September 2009.

[11] Joint Committee of Public Accounts and Audit, Report 417, *Review of Auditor-General's Reports tabled between February 2009 and September 2009*. Parliamentary Paper 163 of 2010, tabled 22 June 2010.

Audit objective and criteria

13. The objective of the audit was to assess the effectiveness of DIBP's management of the CMAL system, having particular regard to the recommendations contained in Audit Report No. 35 of 2008–09.

14. In order to form a conclusion against the audit objective, the ANAO examined the department's:

- strategic approach to the management of CMAL;
- management of CMAL and its implementation of the recommendations of the 2008 audit; and
- management of CMAL stakeholder relations.

Overall conclusion

15. CMAL is a key instrument used by DIBP to manage the entry into and presence in Australia of non-citizens who are of concern for immigration or border security reasons. CMAL information is taken into account when a person applies for a visa to come to Australia, to cross its borders, or applies for Australian citizenship. CMAL contains more than two million records and generates more than 300 000 match cases per month. While CMAL is managed by DIBP, the effectiveness of its operations is affected by, and is important to, the activities of other Australian Government agencies, particularly those concerned with border security, national security and law enforcement such as Customs, ASIO and the AFP respectively.

16. The ANAO's 2008 audit and subsequent JCPAA review encouraged improvements to the administration of CMAL through recommendations relating to the management of the population of the database, data quality measurement and review, performance reporting, quality assurance mechanisms, and the development of policies and procedures for listing Australians on MAL. The audit also noted that DIBP had no strategic plan for managing CMAL.

17. CMAL works effectively at an operational processing level. Centralised data input has seen the overall data quality of CMAL improve, particularly for more recent records and around 92 per cent of records now meet DIBP's minimum data standards. System updates have also delivered improved technical functionality and DIBP's centralised data matching expertise, together with upgraded data matching rules, now provide a high degree of data matching accuracy. DIBP has also developed a close and effective relationship with its key external stakeholders, particularly ASIO and Customs.

18. However, DIBP's strategic management arrangements for CMAL still require development. There has been no strategic planning undertaken to guide the future direction of CMAL nor is there a clearly stated strategic objective for CMAL. Whole-of-government discussions have taken place in recent years to develop an integrated border security alert capability, through the establishment of a National Targeting Centre, that will have ramifications for the operation of CMAL. DIBP also needs to consider how it will manage CMAL in the years ahead for its own immigration purposes. In particular, technological advances in biometrics now make identification of individuals less dependent on biodata and intelligence gathering.

19. While rules for alert reason category (ARC) ownership are set out in the CMAL PAM3, the ownership of CMAL data and consequential responsibility for data quality and integrity are unresolved issues. Addressing these issues, at both the data input stage and through the ongoing review of CMAL records, is important for the operational effectiveness and longer term sustainability of CMAL. Further, until DIBP develops cost effective arrangements to measure CMAL's outcomes and its impact on visa and citizenship decisions, the department will not be in a position to report on the system's outcomes and its contribution to Australia's border security arrangements.

20. In addition, progress in implementing the recommendations in the 2008 audit report has been slow. Of the five recommendations from the 2008 audit, only two recommendations have been implemented. Arrangements for instances where Australian citizens may appear on CMAL (Recommendation 2) are now well managed and subject to regular review. Data quality has improved markedly and CMAL's reliability and client service is regularly measured and reported (Recommendation 4).

21. The status of the recommendations which have not been implemented after more than four years is as follows:

- there is no plan for the population, maintenance and review of the database, although some elements of the plan as recommended have been incorporated into the department's Procedures Advice Manual for CMAL (the CMAL PAM3) (Recommendation 1);

- performance reporting, particularly to demonstrate where CMAL has contributed to the reason for decisions in visa and citizenship applications, is not routinely undertaken (Recommendation 3); and
- systems quality assurance reporting mechanisms have not been finalised. (Recommendation 5). While DIBP now obtains informal assurance that key elements of the interface between DIBP and Customs are operating effectively, agreed formal reporting arrangements between the two agencies remain the subject of negotiation.

22. Given the centrality of CMAL information, there is a compelling case for the department to provide a stronger focus on its strategic positioning, in particular CMAL data ownership and quality control and performance reporting. The ANAO has made four recommendations aimed at strengthening DIBP's management of CMAL.

Key findings by chapter

Strategic planning and management of CMAL (Chapter 2)

23. Strategic planning for CMAL requires DIBP to incorporate two distinct but related considerations: border security activity across government and immigration matters. Border protection is a significant priority for government and CMAL is currently a key feature of Australia's approach. Such activities as the development of an integrated border security alert strategy, culminating in the establishment of a National Targeting Centre, which focuses on passenger risk assessment, will impact on CMAL operations. DIBP will need to be responsive to such whole-of-government initiatives and their potential impact as well as planning for the incorporation of technological advances to keep CMAL sustainable into the future.

24. To date, no strategic plan has been prepared to guide the management and development of CMAL in meeting its border security and immigration objectives. Such a plan would identify the primary purpose of the database and the operational, managerial and technological elements necessary to achieve that purpose. In developing a strategic plan for CMAL, DIBP will need to take into account both the system's expected role in future whole-of-government border security arrangements as well as potential technological developments within DIBP, such as the greater use of biometric technologies.

25. The 2008 audit recommended that DIBP develop a plan to provide for the population, maintenance and review of the MAL database, to which DIBP agreed. The plan was aimed at improving data quality through:

- assigning ownership for data quality;
- the development of rules around populating the database; and
- a review program for alert records and de-activation of those records which were no longer useful.

26. The plan as recommended has not been produced. However, some elements of the intended plan appear in the CMAL PAM3, DIBP's policy and procedures manual for staff.

27. The CMAL PAM3 sets out the categories of Alert Reason Codes (ARCs) as well as the policy guidance and operational rules for each ARC. ARC ownership is formally assigned to the relevant DIBP policy and operational area. ARC ownership includes responsibility for managing the alert records and maintaining the accuracy and currency of the listings. However, in practice, few ARC owners were aware of, or performed, all of their responsibilities.[12] It was only during the audit that DIBP convened a forum for ARC owners so that members could gain a better understanding of their responsibilities and discuss issues of mutual concern with the CMAL systems areas. To meet the requirements of DIBP policies and the intent of the ANAO's 2008 audit recommendation, particularly in relation to the quality of incoming proposed alerts and of existing data holdings, ARC owners should take a more active role in the management of their ARCs.

28. DIBP's management and oversight of the implementation of the 2008 audit's five recommendations was only partially effective. Initially, DIBP sought to establish a CMAL Audit Response Steering Group, but the group was not formally established and no meeting of the group took place. At various times, DIBP provided advice to its audit committee, to the ANAO and

[12] The ANAO conducted a survey of ARC owners to assess their level of engagement with CMAL. The responses to the survey showed that most ARC owners had limited awareness of their responsibilities as ARC owners and did not regularly engage with the CMAL system. Owners of high risk ARCs, such as ARC03, war crimes, were generally more closely engaged with their responsibilities than owners of low and medium risk ARCs.

to the JCPAA, that the recommendations had been wholly or substantially implemented. However, this advice was overly positive.[13]

29. DIBP's audit committee did not make sufficient inquiries to adequately validate management assertions about progress against the recommendations, before ceasing to monitor their implementation. DIBP has advised that its audit committee processes have been amended, with the implementation of a control framework for managing all ANAO recommendations in the future to test the business area's statement that the implementation has been completed.

CMAL data quality (Chapter 3)

30. The 2008 audit found that the 'completeness, quality and currency of MAL data had been an enduring problem for DIAC', principally as a result of the ability for DIBP staff around the network to access MAL directly to propose new alerts and amend or update alert records. This widespread direct access made it difficult for the department to control data quality. Under CMAL arrangements, proposed alerts are submitted by DIBP staff via the Remote Input Function (RIF) and these are checked centrally by the BOC for compliance with minimum data standards (MDS) before listing. DIBP updated its MDS in mid-2011, although data deficient[14] alerts will still be listed if there is a business case to do so.

31. The ANAO's analysis of the CMAL database showed that there has been an improvement in the quality of CMAL records since 2008–09. The department attributes this improvement to the revised MDS and centralised control over alert creation and amendment. ANAO testing showed that only 2.2 per cent of records did not meet the data standards applicable in 2008–09[15], compared with 19.9 per cent of records as at July 2008. DIBP's current MDS impose more stringent requirements than those required prior to September 2011.[16]

[13] As previously noted the ANAO found that only two recommendations had been fully implemented, two partially implemented and one had not been implemented.

[14] 'Data deficient' alerts are those which do not meet the minimum data standards set out in the CMAL PAM3, but which are still listed because there is a degree of risk in not doing so. DIBP subsequently seeks to upgrade the data within the alert through intelligence gathering.

[15] Comparative data testing was undertaken on the copy of the database supplied as at November 2012. The 2008–09 audit undertook data testing as at July 2008.

[16] Based on records active in the database as at November 2012, 92 per cent of all records are compliant with the mandatory standards, and 80.0 per cent with 'desirable' standards. Desirable standards were introduced in 2011 and did not apply prior to that year.

32. DIBP's CMAL records are not subject to any systematic review process even though records may remain on CMAL for lengthy periods (up to 120 years). There are operational benefits in the department developing a review policy and systematic review program, to confirm or expire existing records[17], and to upgrade data deficient records, so that they do not impede the efficient operation of CMAL or cause unnecessary inconvenience for travellers. Older records, which constitute around 80 per cent of all CMAL records, are more likely to be data deficient than records entered since 2011, when the revised standards were introduced. The implementation of an effective review strategy would also assist DIBP to better manage any risks associated with its 'legacy' records.

CMAL performance reporting, management information and systems quality assurance (Chapter 4)

33. The 2008 audit found that there was a lack of performance information to demonstrate CMAL's effectiveness in visa and citizenship decisions, and there was little management information on data quality, client service and system reliability. Despite CMAL's significance to border security, DIBP still does not routinely collect performance information on the role CMAL plays in visa and citizenship decisions.

34. In 2010, DIBP undertook an exercise to assess CMAL's effectiveness in the context of visa and citizenship applications, where it was possible to identify that CMAL information was a factor in the decision making process. This process was largely manual and resource intensive. The exercise identified that, between November 2008 and October 2010, 201 532 individual clients had been matched to an alert. In 78 per cent of these cases (156 520), the decision maker chose not to seek an override and declined the citizenship or visa outcome. In 22 per cent of cases (45 012), the decision maker chose to override the red status and continue the visa or citizenship application process.

35. This exercise provided helpful performance information about the extent to which CMAL information had been a factor in visa and citizenship decsions. However, it has not been repeated and, in the absence of any alternative arrangement, there is no information available to provide insights into CMAL's current contribution to Australia's border security arrangements.

[17] The removal of a redundant record from the database.

While recognising there is a cost associated with collecting such information, there would be benefit in DIBP building on this baseline data and investigating stream-lined and cost effective options for obtaining information about CMAL's contribution to Australia's border security. This information would assist DIBP to better advise the Government and Parliament and also provide a basis for more informed decision making in relation to CMAL. The ANAO notes that for some years DIBP has been attempting to develop its performance reporting capability through the department's business intelligence data warehouse, but completion of the project has stalled. This capability, when completed, would enable DIBP to deliver targeted performance information.

36. DIBP currently reports some management information, principally through routine reports that focus on statistical information and particularly the accurate matching of clients to CMAL data. The monthly statistical report also provides data on incoming, completed and cancelled match cases, the breakdown of completed match cases and the count of true match cases. DIBP also investigates missed matches if and when they come to light. From January 2010 until February 2011, nine missed matches were detected and individually investigated, with reports going to the Secretary and the Director-General of ASIO.[18] In all instances, the missed matches were the result of human error and changes were made to BOC procedures.

37. While there is a balance to be struck between the relative costs and benefits of preparing management information, DIBP could make greater use of CMAL's existing capability to produce more insightful management reports to complement the current data analysis reports. For example, additional reports of potential benefit to management could include analysis of override data, which is where the decision maker, having checked CMAL, decides to proceed with the visa or citizenship application, notwithstanding the information contained in CMAL. The ANAO analysis of override data showed that low and medium risk ARCs were overridden more frequently than high risk ARC alerts, a finding indicative of a system working effectively. The override data also shows that some alerts have consistently high rates of overrides, suggesting that their ongoing inclusion in CMAL could warrant review by DIBP. For example, since 2011, alert matches for debts to the

[18] No further missed matches were detected in the period between February 2011 and October 2013.

Commonwealth have been overridden by decision makers in over 55 per cent of cases.

38. DIBP has sought to integrate CMAL data into its corporate data warehouse[19], to enhance its performance reporting capability. Integration involves a three stage process, with stage one, incorporation of CMAL data, having been completed in 2013. Notwithstanding early advice to Parliament that full integration would be complete by June 2010, stages two and three (integration with other DIBP warehouse data and the development of a new reporting capability respectively), are yet to be funded.

39. External and internal systems quality assurance mechanisms have been put in place for CMAL. A Memorandum of Understanding (MOU) between Customs and DIBP contains an Annex which includes formal system reporting requirements against key performance indicators (KPIs). These formal reports have been under development for several years. Whilst DIBP considers that the current monitoring and reporting arrangements are effective and any systems malfunctions are advised to DIBP within appropriate timeframes, management assurance would be enhanced by implementing the formal reporting arrangements.

40. Within DIBP, the principal systems monitoring mechanism is an Application Monitoring and Reporting Plan, produced monthly and comprising information on CMAL response times and availability of key service delivery webpages, such as adding a PAL or DAL record, assessing a match or searching for a MAL status, to CMAL users. The report provides internal stakeholders, including senior mangement, with performance reports on CMAL transactions against key performance indicators, particularly time responsiveness. Examination by the ANAO of performance reports from January to June 2013 inclusive showed that these reports provided assurance that CMAL is reliable and responsive to users.

Stakeholder management (Chapter 5)

41. DIBP's major external stakeholders are Customs, ASIO, the AFP and DFAT. DIBP's relationships with Customs and ASIO have been formalised in

[19] The data warehouse, DIBP's Business Intelligence Platform, is a data warehouse environment with the associated infrastructure and tools to facilitate the integration of data for management reporting.

MOUs that set out the broad framework of the relationship.[20] The department works closely with ASIO on issues concerned with national security and with Customs on issues concerned with incoming passenger processing. DIBP has formal and informal meetings on a regular basis with Customs and ASIO at strategic and operational levels. Both agencies expressed positive views about DIBP's management of the respective relationships.

42. The department's dealings with the AFP and DFAT are intermittent and focussed on specific ARC categories within the database, such as Interpol listings of serious criminals (AFP), United Nations travel sanctions, war crimes and weapons of mass destruction (DFAT). The department's relationship with these two agencies is in the process of being formalised. The AFP has developed a User Agreement covering the Interpol rules, which is currently with DIBP for its consideration. Formal agreement negotiations are currently being conducted with DFAT.

Managing certain CMAL alerts (Chapter 6)

43. Generally Australian citizens are free to enter and leave Australia at will. However, in 2008, there were 772 Australians listed on MAL. The 2008 audit found that 'the policy on the inclusion of Australians on MAL was not currently coherent or complete'[21] and recommended that DIBP clarify the circumstances under which an Australian citizen is listed on CMAL, update related policy and procedural guidelines and review its holdings of Australian citizens.

44. There are now clear guidelines in the CMAL PAM3 for listing Australian identities and documents on CMAL, as well as specific instructions in each ARC category, advising staff whether Australians can be listed under a specific ARC. Listings of Australians are confined to three ARCs only, national security, organised immigration malpractice and 'surrender Australian travel document'.[22] Further, the department conducts six monthly reviews of Australians on CMAL and by May 2013, the number of Australians listed on CMAL had reduced by 600, to 172.

[20] Detailed arrangements for the management of the IT relationship are contained within the IT annexes to the MOU.

[21] *Op cit*, p. 16.

[22] The 'surrender Australian travel document' is typically a relatively short term category, where Australians who have lost their passports or they have been stolen are listed until DFAT is able to update its passports system.

45. There are also approximately 10 500 children listed on CMAL in all except one ARC.[23] Listings of children arise for generally the same reasons that adults are listed, except for ARC08, child custody concerns. Some listings result from the fact that they are simply a member of a family. For example United Nations travel sanctions will apply to the whole family, and DIBP lists children where there is a debt to the Commonwealth but that debt may have been incurred by a parent. Just over 2 500 children are listed under health concerns and almost 3 000 children are listed under child custody concerns. In addition, 1 315 children are listed on CMAL for debts to the Commonwealth (ARC12).

46. In general, children listed on CMAL will remain on the system for extensive time periods, with only child custody records expiring at the age of 18 years. To manage the potential long-term client service impacts of listing children on CMAL, there would be benefit in DIBP clarifying the circumstances where it is appropriate to list children on CMAL and developing appropriate policy guidance.

Summary of agency response

47. DIBP provided the following summary comment to the audit report:

> My department welcomes the audit as an opportunity to refine the performance of the Central Movement Alert List (CMAL) and further enhance the effectiveness of this vital layer of Australia's Border Security framework.
>
> As part of the multi layered approach to Border Security, CMAL is an integral part of the department's visa and citizenship processing and the key mechanism for identifying potential travellers of concern including national security risks. It is a complex system which is well embedded into Immigration processes and, as identified in the audit, is effective for these operational purposes. The four recommendations are agreed.

48. DIBP's full response is included at Appendix 1.

[23] This exception relates to the ARC covering the surrender of Australian travel documents. In many cases DIBP is bound by legislation or international treaties that do not separately distinguish children from their parents. For example, where the United Nations has imposed travel sanctions, the United Nations and DFAT will require the listing of the whole family, including children.

Recommendations

Recommendation No. 1

Paragraph 2.11

To strengthen the capacity of CMAL as a border security management tool, the ANAO recommends that the Department of Immigration and Border Protection develops a strategic plan to guide and manage the future direction of CMAL in both a departmental and whole-of-government context.

DIBP response: *Agreed*

Recommendation No. 2

Paragraph 2.38

To reinforce to Alert Reason Code owners their responsibility for CMAL data quality, the ANAO recommends that the relevant Alert Reason Code owner reviews proposals to:

- list alerts on CMAL and approves, rejects or requests further information as required; and
- amend and delete CMAL alert records.

DIBP response: *Agreed*

Recommendation No. 3

Paragraph 3.25

To further improve the quality of CMAL alert records, the ANAO recommends that the Department of Immigration and Border Protection develops and implements a regular review program for CMAL records, on a risk management basis.

DIBP response: *Agreed*

Recommendation No. 4

Paragraph 4.21

To better demonstrate CMAL's contribution to Australia's border security arrangements, the ANAO recommends that the Department of Immigration and Border Protection investigates cost effective options for periodically identifying and reporting on those instances where CMAL data has been influential in visa and citizenship decisions.

DIBP response: *Agreed*

Audit Findings

1. Background and Context

This chapter provides an overview of the Central Movement Alert List, its role in border security and immigration activities, and its major stakeholders. Previous reviews and the audit objective are also outlined.

Introduction

1.1 The Department of Immigration and Border Protection (DIBP)[24] manages the entry and settlement of people into Australia. As part of its entry control function, DIBP is responsible for the Central Movement Alert List (CMAL) computer system, an integral component in Australia's whole-of-government, layered approach to border management.[25]

1.2 The primary purpose of CMAL is to alert DIBP's decision makers and external stakeholders to information about an individual during the processing of visa and citizenship applications, passenger and crew processing at overseas check-in points and immigration clearance at the Australian border. People wishing to travel to Australia or those applying for citizenship are checked against CMAL to assess whether they should be permitted to travel to or remain in Australia.[26]

1.3 While DIBP manages and uses CMAL, a number of other agencies and stakeholders either have an interest in its data holdings, contribute to its data holdings or use the data supplied by DIBP in their own border security arrangements.

Overview of CMAL

1.4 Prior to the implementation of CMAL, the Movement Alert List (MAL) was the department's primary database of identities of interest and travel documents of concern, and had been since 1984.[27] CMAL was implemented progressively during 2008 and 2009, predominantly in response to the recommendations of an internal DIAC review, the 2004 Wheen Review, and

[24] The Department of Immigration and Citizenship (DIAC) became the Department of Immigration and Border Protection following the machinery of government changes in September 2013.

[25] DIAC, *Annual Report 2011–12*, p. 147.

[26] Ibid, p.155.

[27] MAL was the subject of ANAO, Audit Report No. 35, 2008–09, *Management of the Movement Alert List*, 21 May 2009.

just prior to the ANAO's 2008 audit of MAL. The department differentiates between CMAL and MAL as follows:

> CMAL is related to the centralised checking of potential matches previously undertaken by DIAC officers throughout the onshore and offshore networks. MAL remains the database from which CMAL checking and database maintenance is performed.

1.5 CMAL comprises two databases, the Person Alert List (PAL) and the Document Alert List (DAL). The PAL database stores the biographical details of identities (biodata) and DAL is a list of lost, fraudulent or stolen travel documents. Heritage MAL (HMAL) is DIBP's legacy and backup system. HMAL was intended to be decommissioned once CMAL was fully operational, but is now used for contingency purposes and statistical reporting, as well as data management and analysis.

1.6 CMAL is managed by the Border Operations Centre (BOC) and the Border Operations Support Section (BOSS) sections of DIBP's Border Operations Branch. The BOC is a 24 hours, seven days per week facility, with responsibility for processing potential match cases in CMAL and supporting DIBP operations and global stakeholders in CMAL related issues. The BOSS provides systems and support capability, including data analysis and performance reporting. It is also responsible for maintaining the CMAL Procedures Advice Manual (PAM3), DIBP's policy guide for the visa, borders and citizenship processing network.

CMAL statistics and costs

1.7 Table 1.1 shows that, in November 2012[28], there were just over 870 000 identities on PAL, equating to almost 720 000 unique individuals, and almost 1.4 million DAL records. On average, almost 33 million potential match cases were considered for the calendar years 2011 and 2012. There were 181 573 incoming match cases per month in 2011–12, with 172 342 true matches[29] being resolved in 2011–12.[30]

[28] DIBP supplied the ANAO with a copy of the database as at November 2012. Statistics discussed in this section are derived from this copy of the database. All ANAO data testing was also undertaken on this copy of the database.

[29] A true match is one which, after consideration by the BOC or policy area, is resolved to be a true match between a visa or citizenship applicant and an alert record in CMAL.

Table 1.1: Key CMAL statistics (as at November 2012)[31]

Key statistics	Numbers
PAL person records	718 276
PAL identities	871 748
Narratives(1)	2 298 365
DAL travel documents	1 375 908
True Matches 2011–12FY	172 342
Non-Matches 2011–12FY	32 722 013
Average Monthly Incoming Match Cases 2011–12FY	181 573

Source: ANAO analysis of CMAL database and DIBP CMAL reporting.

Note 1: Each MAL record has a narrative and may contain several narratives, depending on how often the record has been reviewed or updated. It is a text field and contains the context of the alert listing.

1.8 The full operating costs of CMAL are difficult to quantify given that the management, use and contribution of alerts to CMAL is distributed across a number of areas within DIBP and external agencies. According to information provided by DIBP, total costs for the BOC and the BOSS in 2011–12 were $7 368 922. However, this figure should be considered in the context of the following qualifications:

- DIBP is unable to separate easily the CMAL and non-CMAL related components of these costs, as the teams have responsibilities beyond CMAL;
- the figure excludes the costs incurred by other areas of DIBP that contribute CMAL alerts and use CMAL output, and the time and resources of external agencies that perform similar roles; and
- there are system infrastructure and technical staffing costs incurred by CMAL, which are difficult to isolate because many of these resources are shared with DIBP's other border systems.

[30] DIBP advised that, as at 30 November 2013, PAL contained 683 287 identities, DAL contained 969 320 travel documents and CMAL generated on average 306 509 potential match cases per month, resulting in 174 415 true matches.

[31] Figures have been derived principally from the CMAL database extract provided by DIBP in November 2012, DIBP spreadsheets produced by the DMRT in the BOSS and from DIBP responses to ANAO queries.

CMAL and the travel pathway

1.9 CMAL is an integral part of the travel pathway, with a check of the database being triggered by a person applying for a visa to travel to Australia. CMAL checks are triggered at several points along the traveller pathway, including all visa or citizenship applications, changes to traveller biodata or the addition of other alerts that meet CMAL matching guidelines.

1.10 An anticipated increase in traveller movements will have a direct impact on CMAL operations; the more movements there are, the more visa applications that will need to be processed. Passenger movements (excluding crew movements), have increased from approximately 17 million per annum in 2000–01 to almost 30 million in 2011–12. This number is expected to rise to 50 million per annum by 2020.[32] CMAL will need to have the capacity to meet the challenges presented by these expected demands.

The visa system

1.11 Australia has a universal visa system, which requires non Australian citizens or permanent residents intending to enter or transit through Australia to obtain either a visa or an ETA. Travellers can apply for visas either online or in person, onshore or offshore. Travel agents and airline staff can apply for ETAs on the traveller's behalf.

1.12 DIBP's principal visa processing systems are the Integrated Client Services Environment (ICSE), and the Immigration Records Information System (IRIS). ICSE supports the processing of visa applications from on-shore clients, and visas lodged electronically, while IRIS processes visa applications lodged in-person at DIBP's overseas posts. Visa Processing Officers (VPOs) must consult CMAL to check an applicant's status prior to making a decision on the application. The fact that an individual's details are in the database will not, of itself, mean a visa or citizenship application is refused. CMAL data is one type of information for consideration by the relevant decision makers.

Airline passengers check-in and transit

1.13 The majority of travellers fly into and out of Australia, with small but increasing numbers arriving by ship. Airport staff overseas are required to

[32] DIAC, *Annual Report 2011–12*, p. 145.

enter travellers' details into the airline's electronic check-in system, which interfaces with DIBP's Advance Passenger Processing (APP) system.[33] The APP system checks traveller details against issued visas to confirm that travel is authorised, and also checks against CMAL. Any mismatches between traveller details and issued visas will prevent travellers from boarding until the issue is resolved. The BOC provides around the clock support to airlines to resolve any issues encountered when boarding a passenger. The BOC can give permission for the passenger to board.[34]

1.14 Once a passenger has been processed through check-in, DIBP's Travel and Immigration Processing System (TRIPS) is advised that the traveller is inbound. An Expected Movement Record (EMR) is generated, containing the traveller's flight details, (departure port, expected time and place of arrival)[35], which is forwarded to the Australian Customs and Border Protection Service (Customs). The EMR is confirmed by Customs at the primary line, the CMAL status is checked within DIBP systems and, if required, the status on the EMR provided to Customs is set to 'refer', which will mean the traveller will be referred to a DIBP officer on arrival.

Seaport departures and arrivals

1.15 Seaport departures and arrivals include cruise ships and commercial vessels. All non-Australian passengers and crew require a visa to enter Australia.[36] The procedure for clearing travellers arriving by sea is similar to that for travellers arriving by air. Passengers intending to travel to Australia on maritime vessels are checked against CMAL at the time they apply for a visa, but are not checked against CMAL prior to boarding. Incoming cruise vessels provide details of passengers and crew to Customs at least 96 hours prior to arrival in Australia. This information is checked against the visa record and CMAL.[37] The BOC communicates with the vessel once all passengers and crew

[33] Advance Passenger Processing (APP) is an electronic system that collects information on all passengers and crew, including all transit passengers, travelling to Australia for cross-checking against Australia's immigration databases. Source DIBP, *Australia's APP Advance Passenger Processing System*, 2008, p. 1.

[34] An override may be required in instances where a passenger is travelling on a passport different from that against which the visa is held, where there are typographical errors in the traveller's visa or ETA, and in other instances at the decision maker's discretion.

[35] The movements database contains a detailed history of all travel movements into and out of Australia.

[36] This includes New Zealand citizens, who receive a Special Category Visa on arrival in Australia.

[37] Intercept is a component of Customs' Passenger Analyses Clearance and Evaluation (PACE) system.

are cleared for entry into Australia and transmits the cleared lists to Customs for immigration clearance. Once a cruise vessel docks in Australia, Customs personnel will complete the clearance process and refer passengers and crew with CMAL alert matches to an immigration officer.

1.16 Seaport processing for commercial vessels does not involve APP. The vessel sends Customs a list of crew, which Customs enters into its Intercept system.[38] If there are data or visa issues, a referral report is sent to the BOC to:

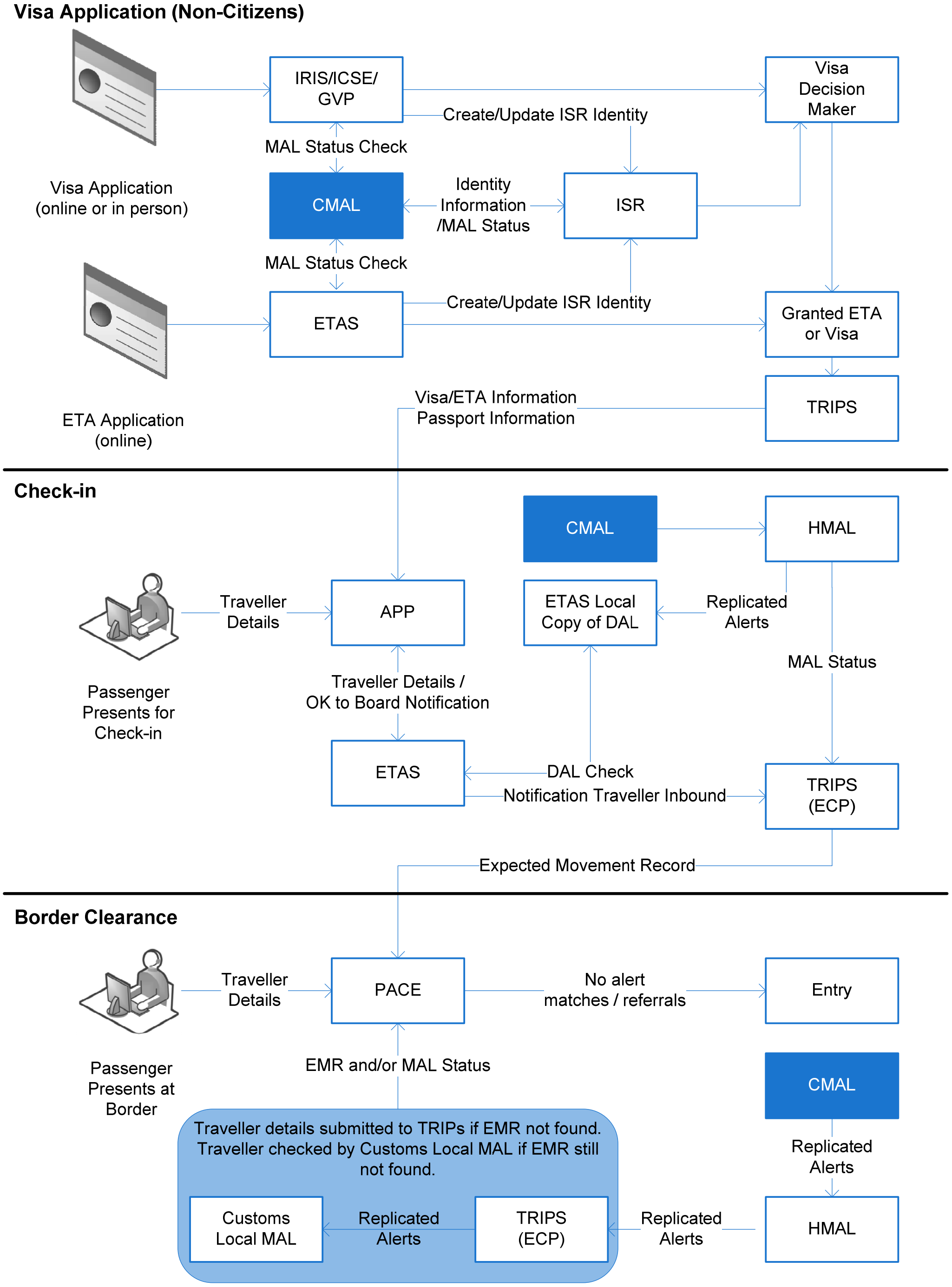
- assess each crew member;
- investigate and correct data issues;
- assess whether there is a valid visa; and
- if necessary resolve any CMAL status.

The referral report is returned to Customs and both DIBP and Customs update their respective systems. When the vessel arrives in port, crew and traveller movements are updated in the DIBP movements database.

1.17 Figure 1.1 summarises the potential traveller interactions with CMAL on the travel/visa pathway.

[38] Intercept is a component of Customs' PACE system.

Figure 1.1: Border systems and the traveller pathway



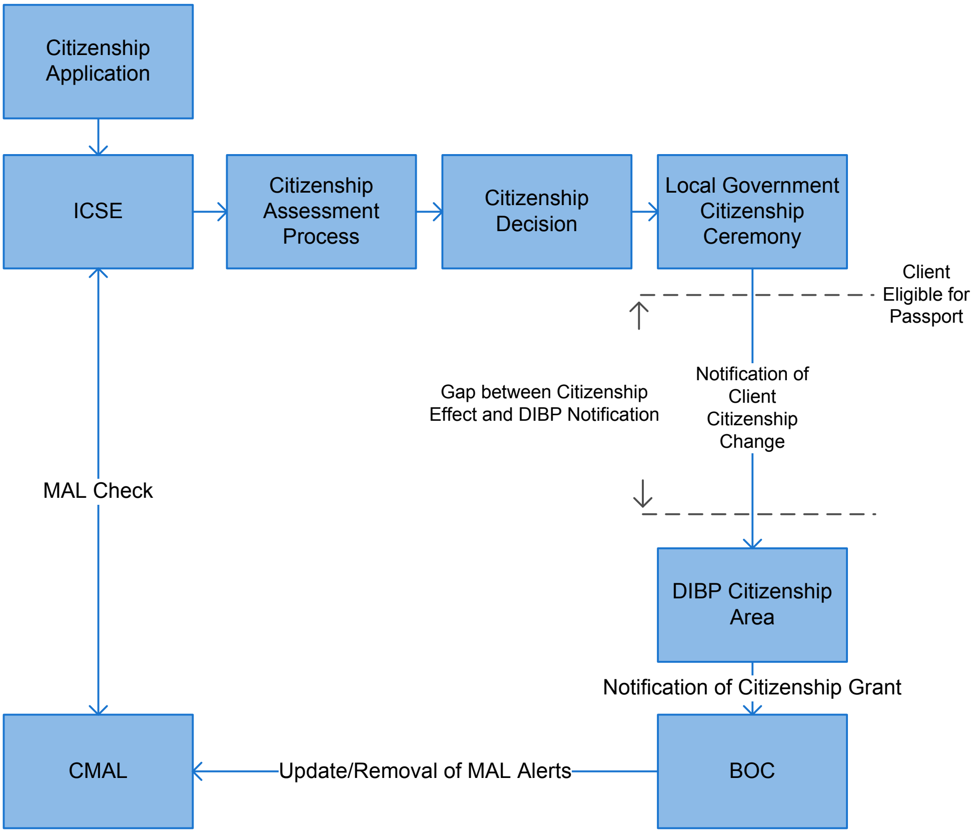
Source: ANAO analysis of DIBP and Customs documentation.

CMAL and citizenship

1.18 In 2011–12, DIBP received 127 400 applications for conferral of Australian citizenship and in 2012–13, 168 822 were received. CMAL's integration for citizenship processing differs from its activities in the travel pathway as there is not the same time-sensitivity around citizenship applications. The service standard for citizenship conferral applications is 60 days for decision making; by comparison, CMAL checks performed for certain visa classes, ETAs, or travellers at airline check-in may need to be resolved in a matter of hours or days.

1.19 Figure 1.2 illustrates CMAL's role in the citizenship process. Applicants for citizenship are checked against CMAL at the decision point for citizenship. CMAL data is one factor to be taken into account and it is up to the DIBP citizenship application decision maker to decide the weight to be given to this information. CMAL is checked immediately before the citizenship decision is made but no further check of the approved applicant against the database is made in the period after this point and up to the conferral of citizenship if the area is made aware of new information during this time.

Figure 1.2: CMAL and the citizenship process


Citizenship Application
ICSE
Citizenship Assessment Process
Citizenship Decision
Local Government Citizenship Ceremony
Client Eligible for Passport
Gap between Citizenship Effect and DIBP Notification
Notification of Client Citizenship Change
MAL Check
DIBP Citizenship Area
Notification of Citizenship Grant
CMAL
Update/Removal of MAL Alerts
BOC

Source: ANAO analysis.

The CMAL matching function

1.20 CMAL manages the alert status of a client, via the PAL and DAL databases. Visa and citizenship applicant data is matched with alerts listed in these databases. The matching function is enabled by specialised software, which undertakes an initial matching process according to computerised rules.[39] CMAL matches are organised into priority queues, that is, the closer a client is to the border, the more urgent the priority and this determines the queue in which the match record is placed. The PAL status options are either red, amber or green: green is a non-match, amber is a potential match yet to be assessed by a CMAL match case analyst, and red is a true match. The DAL status options are limited to red or green; documents either match or they do not. If a client has an amber alert status no decision can be made until that status is resolved.[40] The decision maker must consider a red status and if the decision maker decides to issue a visa or approve a citizenship application, an override code is either provided by the BOC or entered by the decision maker, depending on the risk rating of the alert category.

1.21 The primary purpose of CMAL matching is to maximise the number of true matches between database alerts and travellers or applicants for citizenship, while minimising the number of unresolved matches, which are resource intensive and require the attention of a match analyst. To that end, the chief function of the BOC is the assessment and processing of potential match cases in CMAL, including those time sensitive cases, where a person might be at check-in, approaching the border or at the border. Since the introduction of CMAL, all matching activity is confined to BOC staff, who have been specially trained in conducting match case analysis and assessment.[41] DIBP decision makers around the network can view an alert and the narrative for true match cases, but they do not undertake case matching. An amber alert will require them to contact the BOC for advice and assistance.

[39] Recently, DIBP upgraded its matching engine and matching rules for national security alerts, which are now aligned across government.

[40] 'Resolution' means assignment of an amber CMAL status to red or green.

[41] The centralisation of the CMAL matching function addressed multiple concerns expressed in previous reviews about broad access to MAL and the dispersal of the matching function around the network.

Identity management

1.22 Identity management and the prevention of identity fraud constitutes another important component of DIBP's border strategy. The growth of technology, global trade and international travel has created new opportunities for the evasion of controls at and before the border, and better identity management is assuming greater priority within the department. At present, there is no capability within CMAL to incorporate biometric data and thereby promote a greater degree of certainty in identity management through CMAL.[42]

1.23 Over the past few years DIBP has promoted a biometrics capability as an essential element of risk reduction in the border security space[43], given the limitations of a solely biographic data record system:

> DIAC's long experience of the operation of electronic alert lists demonstrates both the potential and pitfalls of such activities. They are necessarily limited in effectiveness by the need to have either a biographic or (now) biometric alert available, can be limited in effectiveness by poor data, and hence must be buttressed by integrity processes, such as data analysis and profiling, designed to detect 'unknown' threats that fit particular patterns of potential risk. The essence of DIBP experience is that it is not a case of 'either/or', but of alert lists, and other integrity processes, working in concert to achieve an overall reduction in risk.[44]

1.24 The department has been collecting biometric data (facial images and fingerprints) since 2006, principally from people in immigration detention. Biometric data is now also being collected from people applying for citizenship and from offshore visa applicants in 20 countries.[45] The offshore biometric program has been expanded to give airport border officers the capability to verify identity at the border using hand held devices, to 'ensure that the person who provided biometrics at the time of application is the same person entering Australia'.

[42] Identity management is the development of a high level of confidence in the accurate identification of people entering and departing Australia.

[43] DIBP deliverables set out under program 3.1, border management, includes an increase in the use of biometrics (facial images and fingerprints).

[44] DIBP, Annual Report 2011–12, p 149.

[45] As at 29 July 2013.

1.25 However, while biometric data are being collected by DIBP, there is currently no integration of that data within the CMAL database, which remains a collection of biographical data about a person's identity, obtained from a range of sources, of varying degrees of reliability.

CMAL stakeholders

1.26 DIBP maintains the CMAL system for its own purposes and on behalf of other Australian government agencies. Internally, DIBP officers either access the database records in the course of their work or contribute to the database by adding alerts or modifying data. This group includes DIBP staff responsible for issuing visas, airport operations, compliance officers, and onshore and offshore border processing staff.

1.27 Other Australian Government agencies use CMAL for the purposes of border control or to remain informed about the potential presence in Australia, temporarily or permanently, of persons in whom they have an interest. The most significant external agencies with an interest in CMAL are:

- the Australian Security Intelligence Organisation (ASIO) for national security purposes;
- Customs in relation to the processing of incoming passengers/crew at the border;
- the Department of Foreign Affairs and Trade (DFAT) in relation to United Nations (UN) travel sanctions, weapons of mass destruction and controversial visitors; and
- the Australian Federal Police (AFP) in relation to the listing of persons of interest to Interpol.

Previous reviews of MAL

1.28 The MAL database has been the subject of a number of reviews prior to the ANAO audit in 2008–09. Principal among these was the Wheen Review, which reported in 2004. The Wheen Review was wide-ranging and included recommendations to address the following issues, among others:

- poor data quality, including the need to develop a plan to target information sources and put in place 'systemic' arrangements to collect data, and the development of a quality assurance process to monitor the quality of data being entered into MAL;

- the absence of an effective reporting strategy to promote awareness of MAL's performance and to manage the business to achieve optimal outcomes;
- the absence of information about systems performance and data quality and the need for performance reporting to include information on systems operation, data quality, quality assurance;
- the government wide application of MAL and the consequential necessity to establish an inter-agency forum to consider different agencies' interests in the operation of MAL;
- the formalisation of stakeholder relationships, especially those with ASIO, given the substantial interest ASIO had in MAL;
- the lack of policy and procedures for the recording and reviewing of Australian citizens on MAL; and
- identification of the future need for CMAL to have a biometric and image capability.[46]

The ANAO 2008–09 audit

1.29 In 2008, the ANAO undertook a performance audit to assess the effectiveness of the then DIAC's management of MAL, (Audit Report No. 35 of 2008–09, *Management of the Movement Alert List).* The audit identified a number of improvements to the administration of MAL and made five recommendations (set out in Appendix 2) In summary, the recommendations to which the department agreed, were that DIBP:

- develops a plan for the population, maintenance and review of the MAL database (Recommendation 1);
- clarifies the circumstances in which it can properly record Australian citizens on MAL and revises its policy and procedural guidelines for recording Australian citizens on MAL (Recommendation 2);
- improves its reporting on the performance of MAL by identifying instances where MAL has alerted its decision makers to information

[46] David Wheen, *Review of the purpose, architecture and operation of the Movement Alert List (MAL)*, 12 August 2004, Executive Summary, pp. 5-20.

contributing to decisions on visa and citizenship applications (Recommendation 3);

- seeks to measure and report internally on data quality, MAL's reliability and client service (Recommendation 4); and
- implements a mechanism for providing regular assurance that all key parts of the MAL system are operating satisfactorily (Recommendation 5).

1.30 Following the publication of the audit report, the Joint Committee of Public Accounts and Audit (JCPAA) reviewed the audit report as part of its regular review of Auditor-General's reports.[47] The JCPAA recommended that DIBP report back to the Committee after implementing ANAO Recommendation 3 and within six months of the tabling of the JCPAA's report.[48] The Department responded as requested (and this response is discussed further in Chapter 4). Parliamentary interest in CMAL has been ongoing, with DIBP being questioned about CMAL at Estimates hearings on a regular basis.

CMAL audit objective, criteria and methodology

1.31 The objective of this audit was to assess the effectiveness of DIBP's management of the CMAL system, having particular regard to the findings and recommendations contained in Audit Report No. 35 of 2008–09.

Audit criteria

1.32 In order to form a conclusion against the audit objective, the ANAO examined the department's:

- strategic approach to the management of CMAL;
- management of CMAL and its implementation of the recommendations of the 2008 audit; and
- management of CMAL stakeholder relations.

[47] JCPAA, Report 417, Review of Auditor-General's Reports tabled between February 2009 and September 2009. Parliamentary Paper 163 of 2010, tabled 22 June 2010.

[48] Ibid, p.58.

Audit methodology

1.33 The audit team interviewed DIBP staff and internal and external stakeholders, undertook file and document reviews, and qualitative and quantitative analysis of the database and supporting systems.

1.34 DIBP provided a written submission on the status of its implementation of the previous audit recommendations as well as its arrangements with key stakeholder agencies in relation to their interaction with the CMAL system. (Appendix 3).

1.35 The audit was conducted under Section 18 of the *Auditor-General Act 1997* at a cost of $494 429.

Structure of the Report

1.36 The structure of the report is:

Chapter	Chapter overview
Chapter 2: Strategic Planning and Management of CMAL	A strategic plan for CMAL. Managing the implementation of the previous ANAO audit's recommendations. Population, maintenance and review of CMAL.
Chapter 3: CMAL Data Quality	Managing CMAL data quality Quality of current CMAL holdings.
Chapter 4: Measuring and Reporting CMAL Performance	CMAL performance reporting. CMAL management information. CMAL quality assurance processes.
Chapter 5: Stakeholder Management	Australian Customs and Border Protection Service. Australian Security and Intelligence Organisation. Department of Foreign Affairs and Trade. Australian Federal Police.
Chapter 6: Managing Certain CMAL Alerts	Listing of Australian citizens on CMAL. Listing of children on CMAL.

2. Strategic Planning and Management of CMAL

This chapter discusses how DIBP manages CMAL, its strategic approach and the oversight by the department of the implementation of the recommendations of the previous ANAO report. Data ownership arrangements are also discussed.

Introduction

2.1 CMAL has a major role in Australia's border security arrangements. The MAL database was initially developed for immigration purposes, but over the last 10 years, national security has become a focus of government activity, impacting on the operations of the CMAL system. Just over 50 per cent of data holdings and 70 to 80 per cent of CMAL resources are devoted to national security alerts. Consequently, it is important that DIBP's management of CMAL includes the development of appropriate immigration and border security strategies now and into the future.

2.2 The 2008 ANAO audit noted that DIAC had not prepared an overall strategic plan for MAL as envisaged by the 2004 Wheen Review.[49] The department had also not developed a subsidiary plan for populating MAL. The audit report made five recommendations aimed at improving the management of MAL.

2.3 The ANAO examined DIBP's management of the CMAL system, in particular the department's approach to:

- strategic planning for CMAL;
- managing the implementation of the previous audit's recommendations; and
- planning for the population of the database.

A strategic plan for CMAL

2.4 Notwithstanding CMAL's key role in Australia's integrated approach to border security, DIBP still has not developed a strategic plan for CMAL.

[49] ANAO, Audit Report No. 35, 2008–09, op cit, p.38.

There are also few references to CMAL in DIBP's current high-level strategic documents, including the Identity Policy: Principles and Strategies 2013–16, the ICT Strategic plan for 2011–15, and DIBP's Statement of Strategic Intent 2012–15. The business plan for the Global Manager Borders does mention CMAL, but the reference has an operational rather than a strategic focus.

2.5 At various times DIBP has reviewed CMAL and considered potential strategies for its future operations. For example, in June 2010, the then Director of Sustained Operations BOC, produced a draft discussion paper that stated:

> The purpose of this paper is to provide the catalyst and to garnish (sic) senior management support for a courageous and holistic review of the Movement Alert List (MAL). It is designed to drive discussion aimed at determining the Department's and the broader Government's expectations for MAL and to position the capability to more effectively align with a Whole of Government (WoG) biographic and biometric or combined watch list role.

2.6 The audience for this paper is unclear, as is the extent to which the ideas expressed in the paper influenced further discussion. In November 2010, the Executive Committee of DIBP was presented with a strategy paper following a review of CMAL, within which the future direction of CMAL was raised for consideration. DIBP's Executive Committee noted that:

- the CMAL Update and Review identified a number of areas in which the CMAL business model and risk management arrangements can be improved;
- decision points concerning these improvements, commencing with a review of CMAL match display thresholds, will be brought back to EC for approval as necessary;
- the recent progress in improving understanding about the positive impact that CMAL is having on border integrity and national security; and
- CMAL can be developed further as part of DIBP's overall IT roadmap to better support DIBP and other stakeholders.

2.7 The strategic issues raised in the November 2010 meeting have not been further considered within DIBP. DIBP advised in August 2013 that the Executive Committee had not considered any further CMAL matters since February 2011, when the CMAL match thresholds were reviewed and implemented.

2.8 However, a whole-of-government border security strategy continues to evolve.[50] An important element of this strategy is the preservation of Australia's border integrity. Customs chairs a Border Management Group (BMG), which brings together deputy secretaries from 12 border agencies. The BMG is responsible for implementing the Strategic Border Management Plan and coordinating strategic responses to such proposals as a whole of government alert capability. As part of this task, a National Targeting Centre is being considered 'to support an integrated view of air traveller information to enable the identification of high risk air travellers with a greater degree of certainty'. The National Targeting Centre will be initially focused on passenger risk assessment. Its key goals are to:

- allow risk assessment and response planning to be pushed forward of the border;
- integrate the risk assessment processes of border agencies, and
- bring together relevant information and intelligence holdings of border agencies.

2.9 Whole-of-government reforms for border security are under active consideration. It is expected that DIBP will respond to the border security proposals as they are further developed and address the implications for CMAL operations at the appropriate time.

Conclusion

2.10 While high level strategies for border management are clearly articulated in DIBP's public documentation, and the whole-of-government alert strategy is still being developed, a strategic approach to managing CMAL within the department remains unresolved. The development of a strategic plan for CMAL would provide a framework for the management of issues such as enhancing the role of CMAL in an increasingly border security conscious environment and incorporating new technologies, including biometrics for better identity management. A strategic plan would also assist DIBP in guiding and managing the future direction for CMAL in several important ways, including by:

[50] Department of Prime Minister and Cabinet, *Strong and secure:A Strategy for Australia's National Security*, 2013.

- outlining the importance of CMAL in current and future border security arrangements;
- helping to make sure that changes in CMAL, for example, those due to the evolving nature of the database content, technological capabilities and demands for system outputs, are reflected in the department's approach to systems management;
- providing a clearer focus on the management of stakeholder relationships, and associated implications for the sustainability of the system. For example, the number of national security alert records added by the national security agency and the associated workload, has grown significantly in the past 10 years; and
- anticipating the future development of CMAL, particularly in light of new technologies that might enhance the application and effectiveness of the system. For example, DIBP currently has not developed a 'biometric watch list', despite having been funded to do so in the past.[51] Integrating such a capability into CMAL, as recommended by the Wheen Review, would enhance the system's future capabilities.

Recommendation No.1

2.11 To strengthen the capacity of CMAL as a border security management tool, the ANAO recommends that the Department of Immigration and Border Protection develops a strategic plan to guide and manage the future direction of CMAL in both a departmental and whole-of-government context.

Agency response

2.12 *Agreed. DIBP supports recommendation 1 and agrees it is timely after 5 years of CMAL operation to review and refresh our lead agency role for Commonwealth alert list management. The future direction of CMAL will impact across many layers of government, particularly given the impending National Border Targeting Centre and the whole-of-government response to risk.*

[51] DIBP has been considering the potential benefits of biometrics since the late 1990s and received funding of more than $83 million for biometrics initiatives for the period 2003–04 – 2009–10, which included funding for a biometric watch list. ANAO Report No 24, 2007–08, *DIAC's Management of the Introduction of Biometric Technologies*.

Population, maintenance and review of CMAL

2.13 In commenting on the need for a plan for the population of MAL, the 2008 ANAO audit observed that DIBP needed to resolve where the responsibility for the integrity of MAL data lay, with the report concluding that the failure to allocate this responsibility was 'both a persistent and strategic issue'.[52] The report noted:

> The issue of data ownership has long been identified but it clearly requires firm management decisions and action to address it.
>
> 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.[53]

2.14 As a consequence of these findings, the ANAO made the following recommendation (as part of Recommendation No. 1).

ANAO Report No.35 2008–09: Recommendation 1

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.

2.15 The current audit examined:

- the extent to which DIBP has developed a plan for populating CMAL; and
- CMAL data ownership arrangements and DIBP's specification of responsibilities in relation to data ownership and data quality.

A CMAL data population and maintenance plan

2.16 In its response to the 2008 audit recommendation, DIBP agreed to develop a data management plan (DMP), and to review and clarify

[52] ANAO, Audit Report No. 35, 2008–09, op cit, p.15.

[53] Ibid, p.16.

departmental arrangements for MAL data and data quality responsibility.[54] DIBP committed to including in the DMP:

- clarification as to who would be responsible for MAL data, the data quality issues to be addressed and the business rules for addressing them;
- arrangements for data entry into MAL that ensured its own business rules and desired quality standards were observed;
- instigation of a program, with target dates, for data cleansing the existing stock of MAL records; and
- a mechanism for reviewing and reporting progress with this work.[55]

2.17 In the current audit, the ANAO observed that DIBP's primary CMAL reference tool for staff, the CMAL PAM3, states that:

> The overall population and data management strategy for CMAL is defined in the *CMAL Data Management Plan*. This document defines the population, maintenance and review of the MAL database. It clarifies who within the department and externally is responsible for MAL data, the quality issues to be addressed and the business rules for addressing them. It also outlines the arrangements for data entry into CMAL, the data cleansing plan for all MAL records, and how this work is managed.[56]

2.18 The ANAO considers that, *prima facie*, a document of the scope described in the CMAL PAM3 would address many of the key issues embodied in the ANAO's recommendations. However, DIBP advised the ANAO that the document did not exist.

2.19 While the department has not developed the DMP as recommended by the ANAO (and agreed by DIBP), some elements have been developed and promulgated through the CMAL PAM3. These elements include the assignment of responsibility for data ownership (through the Alert Reason Code (ARC) system) and the development of minimum data standards and business rules. However, other aspects of the planned DMP, for example data

[54] Ibid, p.20.

[55] Ibid, p.74 and *Implementation comments on ANAO report recommendations,* DIBP Audit Committee extract.

[56] DIAC, CMAL PAM3, p.10.

cleansing and reporting arrangements, are not contained within the CMAL PAM3.

Data ownership arrangements

2.20 The data ownership arrangements, through the assignment of ARCs, underpin DIBP's data quality arrangements. The PAL database is populated on the basis of these ARCs and has been for many years. The ARCs are 'owned' by the relevant policy and operational areas, generally within DIBP, although other government agencies can also be owners. All PAL alert records must be assigned an ARC and each ARC has a risk category level of high, medium or low. The ARC categories are shown in Table 2.1.

Table 2.1: PAL alert reason codes and risk categories

ARC Number	ARC Name	Risk Category Level
03	War crimes/Human rights abuses	High
04	Controversial visitors/weapons of mass destruction	High
05	Serious or high profile crime	High
06	Health concerns	Medium
07	Organised immigration malpractice	High
08	Child custody concerns	Medium
09	Other criminals	Medium
10	Overstayers	Low
11	Breach of visa conditions	Low
12	Debts to the commonwealth	Low
13	Immigration malpractice	Low
14	Bypassed or refused immigration clearance	Low
16	Suspect genuineness	Low
17	Surrender Australian travel document	Low
18	Travel sanctions	High
19	Illegal fishers	Low
20	False or misleading information/Skilled migration fraud	Low
25	Serious criminal, poor biodata	High

Source: CMAL PAM3, pp. 29–31.

2.21 Conceptually, a system of ARC ownership for data management purposes has been in existence from at least September 2007. DIBP advised that 'ARC ownership as a concept was well entrenched with the concept of MAL, going back to the original PAM3'. Most ARC owners reside within DIBP, with two external ARC owners. Within DIBP, ARC ownership responsibilities are currently divided between policy and operational owners. The identified ARC policy and operational owners are set out in Table 2.2.

Table 2.2: ARC policy and operational ownership

ARC	Policy owner	Operational owner
03	War Crimes Screening Unit	War Crimes Screening Unit
04	Character Policy	Character Operations
05	Character Operations Section	Character Operations Section/BOC
06	Health Policy	BOC/Global Health
07	Intelligence Analysis Section	Intelligence Analysis Section
08	Family Section	Family Section
09	Character Policy	Character Operations/BOC
10	Compliance Policy	Compliance officers in each state and territory office
11	Compliance Policy	Compliance policy
12	Financial Management Operations Branch	Financial Management Operations Branch
13	Intelligence Analysis Section	Intelligence Analysis Section
14	Airport Policy/Detention Operations Support	Airport officers/border intelligence officers
16	Identity Policy	Client Services Group
17	DFAT (covered by Airport policy)	Customs (covered by Airport policy)
18	Character Policy	UN and International Organisations Section/BOC
19	Compliance and case resolution, illegal foreign fisher and logistics	Program Evaluation And Review Section
20	Fraud, Investigations and Prosecutions	Fraud, Investigations and Prosecutions
25	Character Policy	Character Operations/BOC

Source: CMAL PAM3, pp. 33–85.

2.22 As shown in Table 2.2, for eight ARC listings the policy and operational owner is the same (for example ARCs 03, 12 and 13), but for others they are found in separate areas of the department (ARCs 10, 11 and 16). While responsibility is generally assigned to a particular policy or operational owner, for some of the ARCs (such as ARC14) the identified operational owner is a large and disparate group of people, which includes airport officers and border intelligence officers.

2.23 The CMAL PAM3 sets out the responsibilities attached to ARC ownership and these are reproduced in Table 2.3. Generally, policy owners determine the rules and legislative basis for listings, processes for dealing with true matches, identifying credible data sources and setting the threshold score and minimum data standards (MDS) in collaboration with the BOC. Operational owner(s) manage records, hold evidence for listings and make decisions on any match cases referred by the BOC. The Border Operations Support Section (BOSS) also plays an important role in providing systems support for CMAL functions and in managing the CMAL PAM3, although no mention of the section is made in that document.

Table 2.3: ARC policy and operational owner responsibilities

Policy owner defines:	Operational owner:
Policy and rules for the record set	Manages a set of records in the ARC
Credible data sources	Holds the evidence for each record listing
Legislative basis for the alert	Deals with requests to clarify match case referrals
How the match is confirmed	Liaises with the information sources
Referral procedures	Maintains the accuracy and currency of the MAL records
Where evidence supporting the record can be located	
Processes for a red status	
The match case threshold score	
Minimum data standards for the ARC	

Source: CMAL PAM3, pp. 32–33.[57]

[57] In the February 2008 version of the PAM3, the responsibilities of ARC ownership were largely consistent with those in the current CMAL PAM3: ‘The business area requesting the MAL listing has ownership of the particular Alert Reason Code (ARC) (reasons for listing) and the source of information. The business area is responsible for providing policy advice to DIBP staff and other agencies when there is a possible MAL match and is also responsible for control of the data quality. In addition, the business area is solely responsible for the integrity of the biodata and narrative recorded in the records for listing.’

2.24 While each ARC is owned by a particular area, DIBP staff generally can propose new alerts and modifications to existing alerts through the Remote Input Function (RIF). The BOC, and not the ARC owner, reviews the alerts proposed through the RIF to ensure that:

- the reasons for the listing are in line with policies for inclusion in CMAL;
- the data quality standards have been met; and
- the necessary approvals have been sought.

2.25 Once approved by the BOC, the alert is then formally created within the CMAL database. One of the consequences of this approach to populating CMAL is that, while ARC owners are expected to exercise responsibility for data management, they are not part of the chain of approval for proposed alerts and cannot exercise quality control over those alerts.

2.26 In February 2013, DIBP noted in its submission to the ANAO the significance of the ARC system as a mechanism for ensuring data quality through ARC ownership responsibilities:

> Alerts were split into Alert Reason Codes (ARC) with appropriate ARC owners identified across DIAC. Each ARC owner is responsible for managing their own alerts and the relationship with stakeholders who provide input to the alerts. They also have responsibility for the creation of alerts using the Remote Input Function (RIF) which was implemented in November 2010. Alerts are created by the area with an understanding of the business but requiring approval by the BOC to ensure alerts met requirements for that ARC along with data quality standards.

2.27 While the BOC currently has responsibility for reviewing proposed alerts to ensure the alert meets CMAL PAM3 guidelines, the department does not measure how effectively the BOC undertakes this activity.

ANAO ARC owners survey

2.28 The ANAO's initial discussions with ARC owners suggested that many were unfamiliar with their CMAL responsibilities and considered activities relating to CMAL to belong with the Border Operations Branch. The ANAO also surveyed ARC owners in order to assess the extent to which they understood their responsibilities. ARC owners were asked the following questions:

- What does your area do when you want to add a record to MAL? What procedures exist in your section to guide staff in this activity? and
- What does the area do in reviewing existing records for currency, accuracy?
- If you have any guidelines or procedures in your area around this activity please provide a copy.

2.29 Completion of the survey was complicated by the fact that DIBP's ARC ownership list was not up-to-date. Ultimately, 18 ARC owners were contacted, with responses received from 17 owners. The major findings from the survey were:

- while ARC owners were generally aware of the mechanisms for proposing alerts, there were 15 ARCs for which there was no regular review process in place. Records were removed when requested by an external agency or were reviewed in response to a request from the Border Operations Branch. Only two owners (ARC07 and ARC13) reviewed their holdings on a regular basis, and ARC07 records were reviewed only in relation to Australian citizens;
- there was a high level of awareness of the CMAL PAM3, which was the primary document used by DIBP staff to access and input data into CMAL. Three ARC owners also had local guidelines to assist staff; and
- there was no mechanism in place to alert a new occupant of a position to CMAL ARC ownership obligations. Consequently, the ARC10 and ARC11 owner was unaware of any responsibility for CMAL data, having been newly appointed to the position.

2.30 Overall, the survey indicated that ARC owners had a limited understanding of the obligations inherent in their role. These findings are confirmed by the minutes of two meetings held by the Border Operations Branch with ARC owners in March and June 2013. (see paragraph 2.33)

ARC Owners Consultative Forum

2.31 In 2009, DIBP advised the ANAO that it would be establishing a replacement group for a disbanded MAL Practice Management Group, to progress data ownership and quality matters.[58] However, it was not until March 2013, almost four years later, that an ARC Owners Consultative Forum was established.

2.32 The forum was convened to 'provide opportunities for information sharing across the different business divisions and to ensure that decisions made by the Border Operations Branch were well informed and appropriately risk managed'. Draft terms of reference for the forum include to:

- provide opportunities for information sharing across different business divisions and agencies;
- provide feedback to ARC owners on operational issues experienced in the borders environment, including the Border Operations Centre;
- discuss data quality issues and identify areas for improvement;
- raise and resolve emerging risks and issues;
- ensure that business-as-usual activities are 'best practice' and aligned with other departmental initiatives and systems.

2.33 The forum is chaired by the Assistant Secretary Border Operations Branch and includes representation from the key business areas responsible for the administration of ARCs within DICP. The first meeting was held on 26 March 2013 and a second meeting on 26 June 2013. The minutes of the first two meetings confirmed that the ARC owners were unfamiliar with several aspects of CMAL operations, specifically:

- the respective roles of the BOC/BOSS and ARC owners;
- the alert listing process; and
- reviewing, amending and deleting records.

2.34 The establishment of the forum is a positive step and will provide a structure for better collaboration between ARC owners and the Border Operations Branch. It will also enable ARC owners to be more engaged with CMAL processes, in particular, review of alert records with poor biodata and obviously redundant records. However, to be effective, the forum will require continued support and oversight from senior management to promote an ongoing commitment to this activity.

[58] ANAO, Report No, 35, 2008–09, op cit, p.45.

Conclusion

2.35 The 2008 audit recommended the development of a plan for the population, maintenance and review of the MAL database and clarify in that plan where the responsibility for MAL data lay. DIBP has included in its CMAL PAM3 aspects of the recommended DMP, such as ARC ownership arrangements for PAL data records and business rules, including minimum data standards for listing data records. However, the data cleansing and reporting arrangements have not been developed and DIBP has not produced a plan for the population, maintenance and review of the database as recommended by the 2008 audit and agreed by the department.

2.36 DIBP has articulated in the CMAL PAM3 a system of ARC ownership, with identified responsibilities for policy and operational owners. However, generally speaking, current ARC owners, until recently, have been largely unaware of the scope of their responsibilities for managing CMAL data and consequently did not perform the full range of their responsibilities.[59] Until recently, there has also been no mechanism for the Border Operations Branch to engage formally with ARC owners. Further, the limitations on the involvement of ARC owners in alert development and oversight of proposed alert holdings, has both precluded them from taking active responsibility for the quality of alerts and hindered their ability to manage data quality, outside the setting of data standards and policy parameters.

2.37 Responsibility for CMAL data quality is currently a shared responsibility between the BOC, BOSS and ARC owners. Their respective roles require clear articulation in the CMAL PAM3 to promote broader understanding of their roles by departmental officers. In particular, there would be benefit in amending the RIF procedures for proposed alerts, so that responsibility for approving the listing of these alerts in CMAL resides with the ARC owners where the policy expertise underpinning data quality is to be found. This change will enable the BOC, the repository of data matching expertise, to concentrate its resources on resolving match cases.

[59] ANAO analysis. ARC owners were surveyed in March 2013 to determine the level of current engagement with management of their ARCs.

Recommendation No.2

2.38 To reinforce to Alert Reason Code owners their responsibility for CMAL data quality, the ANAO recommends that the relevant Alert Reason Code owner reviews proposals to:

- list alerts on CMAL and approves, rejects or requests further information as required; and
- amend and delete CMAL alert records.

Agency response

2.39 *Agreed. DIBP has been working with Alert Reason Code owners to improve their understanding of their responsibilities as owners and increase their knowledge of relevant Alert Reason Codes. The Alert Reason Code Owners Forum has established regular meetings, is fostering relations and sharing information about CMAL functionality and improvements.*

Managing the implementation of the previous audit's recommendations

2.40 As discussed earlier, the previous ANAO report made five recommendations, as well as a number of suggestions for administrative improvements. DIBP's initial response to the ANAO's audit of MAL was to establish a CMAL Audit Response Steering Group, intended to oversight the department's response to the audit's recommendations. In November 2009, a minute was sent to key departmental stakeholders proposing the formation of the steering group. The envisaged scope of the group was to encompass changes to policy advice on the use of MAL, improvements in data quality management practices, and improvements in reporting and systems monitoring. An inaugural meeting of the group was originally scheduled for the end of November 2009, but was postponed due to a lack of response to the BOC email. Subsequently, on 26 November 2009, a follow up email was forwarded to stakeholders in an attempt to encourage them to become involved in the CMAL exercise:

> … we are also holding some internal workshops to review what MAL is all about, and to develop some new models for determining the role and responsibility of the [Alert Reason Code] (ARC) owners. We are doing this so that we can come to the Steering Group with some options for modernising the capability. One option could be greater centralisation of the maintenance of the MAL and much clearer delineation of the roles and responsibilities of the ARC

> owner group as opposed to my operations effort. The Steering Group is a great opportunity to influence the way ahead for the management of the MAL.

2.41 No meeting of the steering group eventuated, and no similar structure with responsibility for progressing the implementation of the recommendations was established.

2.42 DIBP has provided advice as to the status of the implementation of the previous audit's recommendations on several occasions. In October 2010, DIBP's audit committee, which is responsible for monitoring the implementation of internal and external audit recommendations, received advice that three of the recommendations had been addressed, and that two were in the process of being addressed. No review was conducted nor was supporting evidence sought to validate the advice. Consequently, all five recommendations were considered to be completed or closed, and monitoring by the audit committee ceased. In February 2013, at the commencement of the current audit, DIBP stated that four of the five recommendations of the previous audit had been fully addressed, while the fifth (Recommendation 3) was currently being addressed and the focus of continuing work.

2.43 The absence of an effective approach to managing and monitoring the implementation of an audit or review's recommendations carries with it the risk that appropriate remedial actions may be commenced, but not completed, or not commenced at all. Senior management may, in these circumstances, form an unduly positive view of progress due to a lack of visibility over implementation actions within the department. Given the complexity of CMAL operations and its parliamentary profile, more focussed senior management oversight could have been directed to the implementation of the recommendations.

Conclusion

2.44 It is the ANAO's assessment that the implementation of the recommendations is less complete than previously advised by the department. Appendix 2 summarises the ANAO's assessment of the department's progress in implementing the recommendations. Of the five recommendations, two have been implemented, two have been partially implemented and one has not been implemented.

2.45 DIBP has since advised that amended procedures have been put in place to monitor the implementation of the ANAO's recommendations, as follows:

The Department has implemented a control framework for managing all ANAO recommendations in the future to test the business area's statement that the implementation has been completed. As a part of the closure process, responsible First Assistant Secretaries will identify the specific action(s) that have been undertaken, what evidence will demonstrate that the results of implementation have been realised, when will the evidence be available and where will the evidence be recorded. Prior to and post closure, Internal Audit will be able to verify that supporting evidence exists.

An example is that a policy is promulgated in response to a recommendation. The date of implementation would be the date of promulgation. Post implementation evidence would be a change of practice evidenced in the business areas, seen as a result of quality assurance measures that were taken, for example, three months afterwards.

3. CMAL Data Quality

This chapter discusses DIBP's processes for maximising data quality through the development of business rules, minimum data standards and review processes, and assesses whether data quality has improved since 2009.

Introduction

3.1 The quality of CMAL's data holdings is fundamental to the effective operation of the CMAL database. 'Quality' refers to the accuracy, currency and relevance of the data. The more accurate and relevant the data, the more effective the database. Retaining only relevant holdings in the database enhances operational efficiency in terms of database matching.

3.2 The 2008 audit noted that 'the completeness, quality and currency of MAL data has proved an enduring problem for DIAC'. The report further noted that previous reviews of MAL had stressed the importance of sound data, but that, despite efforts to improve MAL data, overall data quality had been declining.[60] The ANAO made the following recommendation:

> As part of Recommendation No. 1, the audit recommended that the plan for the population, maintenance and review of the database include:
>
> - 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.

3.3 This audit examined:

- DIBP's procedures for managing and reporting CMAL data quality through business rules and minimum data standards; and
- the quality of current data holdings and changes in data quality since the earlier audit report.

[60] ANAO, Audit Report No. 35, 2008–09, op cit, p.14.

Managing CMAL data quality

3.4 Quality CMAL data requires not only good ARC management processes but also the application of business rules and minimum data standards (MDS). The development of business rules for new alert records increases the chances that the record will be based on appropriate information from a recognised source, that is, it will be relevant and accurate. The application of MDS will also help to ensure that data fields contain the required data content.

3.5 In July 2010, DIBP commenced a strategy to revise the MDS for each ARC alert 'to improve the standard of CMAL records and to reduce the number of poor quality potential match cases created by these records'. The revised MDS were implemented in September 2011. DIBP also created a set of business rules within each ARC for the guidance of ARC owners and proposers of alerts.[61] These are set out in the CMAL PAM3.

Business rules and minimum data standards

3.6 Business rules express 'a policy or condition that governs business actions and established data integrity guidelines'.[62] The ARC business rules set out in the CMAL PAM3 comprise both policy and operational instructions, including the minimum data standards to be applied to each ARC. The rules set out the policy basis for the ARC, identify the ARC owners and their responsibilities and provide for acceptable sources of information, among other things. The operational business rules, which differ by ARC, govern how alerts are added, managed and responded to. The rules also describe the information necessary to populate an alert for each specific ARC, when and how alerts should be reviewed or expired, and desired actions in the event of a match. For example, for ARC03 the business rules require that potential matches are referred to the ARC owner for resolution.

3.7 MDS are defined as 'the minimum amount of data that is necessary to create a record that is considered to be complete'. MDS may include

[61] National security alerts are not relevant to this discussion. DIBP MDS are not applied to national security alerts, to which different data standards apply.

[62] DIBP refers to CMAL business rules as 'system constraints'. However this term is misleading because the matters listed are not system constraints, as there is no system imposed barrier to data entry if data outside the parameters listed is entered into the system. What DIBP refers to as system constraints has been interpreted by the ANAO as business rules and DIBP has agreed to these definitions.

requirements for those parts of the record that must contain data and the types of data that are considered acceptable. For example, ARC07 (organised immigration malpractice) contains the following mandatory fields: family name, year of birth, gender/sex, country of birth or citizenship (at least one) and informer. More rigour is imposed on certain other categories, including for example, ARC11 (breach of visa conditions) where the following fields are mandatory: family name, given name, date of birth, gender/sex, country of birth, citizenship and informer.

3.8 While the MDS represent the minimum standard DIBP requires of its CMAL records and staff are encouraged to provide as much information as possible, there are good reasons for permitting the listing of some data deficient records. The challenge for DIBP in setting the MDS is to permit the listing of those records which include sufficient information for a decision maker to make an informed decision on a match case, while at the same time seeking not to omit records which might be a potential match to an alert, without listing alerts which are so data deficient as to compromise the effectiveness of the database.[63]

3.9 DIBP is flexible in the application of the MDS, allowing alerts which do not conform to the recommended MDS to be listed if the proposer can make a business case for the listing. For example, alert owners such as DIBP's war crimes unit choose to include data deficient alerts rather than potentially miss a true match in a high risk category. The inclusion of these alerts will result in a higher number of match cases and more work for the BOC and the ARC owner. However, the listing of data deficient alerts also reduces the chances of missing a true match, a significant factor for owners of high risk alerts.

Mechanisms for promoting compliance with the MDS

3.10 To promote compliance with the MDS, the department's strategies include the provision of business rules and the listing of alerts through the RIF with oversight by the BOC, prior to the alert record being listed on the PAL database.

[63] Requirements for each data field vary by ARC; the MDS for the immigration related ARCs are more stringent than those for an ARC such as ARC03, war crimes. In some instances a field may be listed as 'desirable', indicating that, while not required, data should be entered if available.

3.11 DIBP refers to the MDS and business rules as 'system constraints', suggesting enforcement of these requirements within the CMAL system itself.[64] In practice, only selected rules and MDS are constrained by the CMAL interface, and most may be overridden if a business case exists to do so.[65] DIBP advises that the system has been designed to be relatively unconstrained, in order to enable the listing of alerts with poor data quality, either temporarily until the data quality issues can be addressed or more permanently, because in the judgement of the proposer, the alert needs to be listed irrespective of data quality.[66] Consequently, while DIBP expects its staff to take notice of the business rules and MDS when proposing alerts, the primary method of constraint is not system imposed, but rather through the review of new (proposed) alerts by BOC staff.[67] DIBP advised the ANAO that approximately one per cent of proposed alert entries are rejected. These could be new alerts, amendments or requests for deletion; the CMAL system does not record these categories separately.

3.12 The Data Management and Reporting Team (DMRT) in the BOSS produces a monthly error report on newly listed alerts. The report identifies MDS errors in PAL and DAL alerts which have come through the RIF and been listed on CMAL. PAL errors identified can include family and given name errors such as 'Unknown' or 'no family name'; titles such as 'Mr' or 'Dr'; and alerts where the person is Australian under a non-compliant ARC or where no formal approval has been provided. The monthly error report therefore provides a measure of quality assurance of the BOC review of proposed alerts. While the DMRT does some limited review of the PAL narratives in the course of producing the montly RIF report, these narratives are not systematically reviewed (discussed in Chapter 4) and identified DAL errors are limited to

[64] Generally speaking, a 'system constraint' is where a system imposes a barrier on the entry of data that falls outside of specified parameters. For example, if the data field requires that a date be entered, the system may apply rules associated with that date (such as preventing the recording of an alert where the date indicates that the person is a child, if it were not acceptable for children to be listed under that ARC).

[65] For example, individuals considered to be of high-risk but for whom limited information is available may be added immediately, with the proviso that additional data be added to the alert as it becomes available.

[66] There is a legislative compulsion for DIBP to list certain records irrespective of data quality. In particular, they must list persons against whom UN travel sanctions have been imposed and the families of the primary identity. Often, DIBP will not receive full details of the persons concerned, but must still list whatever detail is supplied by DFAT. DIBP advised that, where possible, it will revisit these data deficient alerts and attempt to obtain further information to make them more compliant with the MDS.

[67] Paragraphs 2.28, 3.10 and 3.11 describe the role of the BOC in the review of proposed alerts.

such major errors as the omission of required text in the narrative for listings of Australians.

CMAL data maintenance

3.13 As the 2008 report noted, 'MAL records are unlikely to be useful in perpetuity'.[68] Once entered via the RIF and approved by the BOC, the stock of CMAL data holdings requires ongoing maintenance to:

- identify records with poor biodata and either add the data necessary to bring them up to the MDS or delete data deficient records, thereby cleaning up the database; and
- 'expire' records which are no longer relevant for retention on the database.[69]

3.14 The ANAO examined the extent to which DIBP reviews data deficient records and cleanses records which are no longer relevant for retention on the database.

DIBP's review and expiry rules

3.15 The ARC rules in the CMAL PAM3 contain a policy instruction for a review of the alert as well as default review and expiry dates. The varying policy requirements and default review/expiry dates for each ARC are set out in Table 3.1.

[68] ANAO, Audit Report No. 35, 2008–09, op cit, p. 62. Under the current privacy principles, there is also a privacy imperative to review data on individuals held by an agency. A Privacy Impact Assessment, conducted in 2010, noted that the BOC, as managers of the CMAL process, should provide strategic guidance to the owners of the data on CMAL, to ensure a regular process of review is conducted to update information held in CMAL which is deemed of lower accuracy or from a lower quality source, to ensure the accuracy of information held.

[69] 'Expiry' of a record deactivates a CMAL alert associated with a person, although the records remain technically on the system, with access limited to DIBP staff with special permissions.

Table 3.1: Policy requirements for review and CMAL default expiry and review dates

ARC no	ARC title	Review policy	Default review and expiry dates set by CMAL (D = expiry; R = review)
03	War crimes/human rights abuses	10 years from create date	D120 (age of client) R 10 (from create date)
04	Controversial visitors/weapons of mass destruction	10 years from created date	D120 (age of client) R 10 (from create date)
05	Serious or high profile crime	1 month from create date, extension with approval Expire at 100 years of age or on attainment of Australian citizenship	D100 (age of client) No default review date
06	Health concerns	Periodically CMAL data management team will assess narratives against group codes	D120 (age of client) No default review date
07	Organised immigration malpractice	10 years from create date Expire at age 100 if convicted of people smuggling	D100 (age of client) R 10 (from create date)
08	Child custody concerns	At 18 years of age If record based on allegation within 1 month, extension approved by CMAL client services	D18 (age of client) No default review date
09	Other criminal	Allegation – 1 month from create date, extension approved by CMAL client services If FATA, expire alert in 10 years Expire at 100 years or on attainment of citizenship	D100 (age of client) No default review date
10	Overstayers	3 years from departure date/create date	D3 (from create date) No default review date
11	Breach of visa conditions	3 years from date of visa cancellation	D3 (from create date) No default review date
12	Debt to the Commonwealth	>$1000 – 10 years from date of departure/create date <$1000 – at age 100 years Can be expired if paid	D100 (age of client) No default review date

ARC no	ARC title	Review policy	Default review and expiry dates set by CMAL (D = expiry; R = review)
13	Immigration malpractice	3 years from departure date/create date	D3 (from create date) No default review date
14	Refusal/bypass immigration clearance	3 years from departure date/create date	D3 (from create date) No default review date
16	Suspect genuineness	3 years from departure date/create date	D3 (from create date) No default review date
17	Surrender Australian travel document	Review 1 month after listing Expire 12 months after create date	D1 (from create date) No default review date
18	Travel sanctions	Review 5 years from create date	D120 (age of client) R5 (from create date)
19	Illegal fishers	Expire 5 years from create date	D5 (from create date) No default review date
20	False or misleading immigration/skilled migration fraud	Delete 3 years from date of visa refusal	D3 (from create date) No default review date
25	Serious criminal – poor biodata	Review 2 years from create date or update to ARC05 if more biodata	D100 (from create date) R2 (from create date)

Source: CMAL PAM3, pp. 34–85.

3.16 In order to maintain the integrity of the CMAL database, DIBP procedures provide for review and expiry of alert records. Review of a record can be as a result of new information coming to the attention of DIBP or the review period is stated in the alert record. Departmental officers in the network or ARC operational owners can review listings, depending on the reason for the review. Review and expiry of alert records means the archiving of the record and not permanent deletion.[70]

3.17 If no review date is specified in the proposed alert, the CMAL system automatically sets a review date for each listed identity based on the ARC under which it is listed. If no default review date exists, the alert will expire in accordance with the default expiry date. The CMAL PAM3 does not specify

[70] Once inactive, records cannot be amended. Further, only certain BOC staff are able to access inactive records.

the basis on which particular ARC review dates were determined. The CMAL system settings have not been amended since CMAL was implemented and DIBP advises that, because there has been no trigger for a review, the settings have remained unchanged.

3.18 CMAL will automatically expire alerts falling due on a particular day and, where possible, ARC policy and operational owners are encouraged to set automatic expiry dates for identities. However, the PAM3 manual does not identify whether it is the policy owner or the operational owner who has the responsibility for setting the expiry date.

3.19 Some ARC alert records have relatively short term expiry periods, such as ARC19 (illegal fishers) alerts, which automatically expire after five years. However, most ARCs have lengthy expiry periods, often 100 years from the creation of the record or at 120 years of age. Where there is no MDS for review and expiry, then the alert will be listed without proposed review and expiry dates. The alert will therefore remain on the system for the default expiry period.

3.20 Following a systems change in March 2013, DIBP now has the capability to identify by ARC, those alerts which are about to expire or which need review. The ANAO considers that this functionality will be important in prompting ARC owners to review their data.

Cleansing CMAL data

3.21 The regular review of CMAL records assists in maintaining records which are current and accurate. Generally, ARC policy owners set the MDS and the operational owners are responsible for maintaining the accuracy and currency of the CMAL records. Consequently, the review process is an important means by which operational owners can exercise their responsibility for data cleansing. While PAM3 states that CMAL will prompt the ARC operational owner to review a record when it is due, DIBP has advised that this prompt does not occur. There is a systems change to enable this facility, which has not yet been scheduled. Rather, a recent update to the CMAL system has been the development of a 'date search' capability, that allows users to identify alerts by ARC, which are due to either expire or to be reviewed. CMAL does not monitor review activity *per se* and it is therefore not possible for DIBP to monitor if an alert record has been reviewed, unless alerts are updated or amended.

3.22 During the audit, the ANAO observed that review activity is generally ad hoc and in practice, ARC owners review their data when prompted by the Border Operations Branch or on request from an external agency, such as DFAT. Alert records might also be reviewed incidentally, as a result of new information coming to light, either via a DIBP staff member in the network or through the BOC. Only two ARC owners maintain a proactive program of data cleansing. ARC03 (war crimes) records are systematically reviewed on an ongoing basis. The War Crimes Unit has a detailed local procedure for checking the records, amending the narrative and the appropriate action to be taken in relation to an alert. The ARC07 (organised immigration malpractice) owner reviews the alerts for Australians on CMAL, but there is no process to review all ARC07 alerts as a matter of routine.

3.23 While ARC owners are expected, individually, to maintain their data holdings, DIBP also sought to commence a centralised data cleansing strategy as part of the implementation of amended MDS in June 2011. For the majority of ARCs, a minute containing a list of the 300 most problematic alerts for that ARC was distributed to ARC owners. DIBP advised that there was a 'limited response' from ARC owners, but that those who responded were provided with assistance. DIBP was not able to provide evidence that the promised contact and subsequent development of a review policy occurred. DIBP's review of legacy holdings remains at an early stage of development, as noted by DIBP in its February 2013 submission:

> The BOC continues to work with the alert reason code owners to review their legacy holdings in MAL. Currently ASIO receives a monthly report that outlines the most problematic (from a data quality perspective) 300 national security alerts. This process is being developed for all the remaining DIBP ARC owners to undertake similar work. This will progressively remove the poor quality records or force the addition of more biographic data to improve overall data quality.

Conclusion

3.24 The ANAO considers that the introduction of business rules and revisions to the MDS for CMAL are positive steps in the ongoing development of the CMAL system. Centralisation of the review of proposed alerts also provides a platform for greater consistency in the content and quality of alerts. In addition, the RIF error report provides a measure of quality assurance for BOC review of proposed alerts. However, the department has not developed a review program for alert records, nor is there a program of data cleansing of the existing stock of database records. Therefore, no mechanism for routine reporting on this aspect of CMAL operations exists, as proposed in ANAO Recommendation No. 1.

Recommendation No.3

3.25 To further improve the quality of CMAL alert records, the ANAO recommends that the Department of Immigration and Border Protection develops and implements a regular review program for CMAL records, on a risk management basis.

Agency response

3.26 *Agreed. The Alert Reason Code Owners Forum has been used to highlight the issue with alert owners. Minimum Data Standards for alerts will be reviewed to ensure that data flowing into CMAL is of the highest possible quality. Systematic reviews of data will be undertaken by Alert Reason Code owners to ensure that alerts in the system with a long lifespan remain relevant, accurate and provide value to DIBP decision makers.*

Quality of current CMAL holdings

3.27 In order to test the current state of CMAL data, the ANAO obtained a copy of the CMAL database, comprising the complete set of PAL and DAL records, associated narratives, ARCs and informer data. The ANAO replicated as far as possible the testing undertaken by the Wheen review and the 2008 audit in order to assess firstly, whether DIBP's data quality had improved over time and secondly, to examine the current state of MAL data quality against the requirements of the amended MDS, which took effect in September 2011.

Improvements in data quality over time

3.28 The ANAO considered MAL data at time points 2003 (the Wheen Review), 2008 (the ANAO MAL audit) and November 2012 (the date at which DIBP provided a copy of the CMAL database to the ANAO). To assess the extent of improvement in data quality over time, ANAO testing analysed data by ARC category, at each time point and included the proportion of:

- data deficient PAL records within the PAL database;
- data deficient high risk PAL records within the PAL database; and
- data deficient PAL records not including national security records.

3.29 The criteria used to assess the records were those established by the Wheen Review by which an alert would be deemed deficient, focusing on the absence of key pieces of biodata. Because of changes to the structure and business processes of CMAL, some elements of the Wheen tests have been rendered less relevant and consequently qualify the results to some extent. The implications of the differences are:

- CMAL does not distinguish between primary and secondary ARCs as was possible in the previous system, when alerts could be categorised against a primary ARC and also against additional secondary ARCs. For this reason the production of statistics of compliance by ARC category is less meaningful, due to the earlier possibility of double-counting records with multiple ARCs; and
- the 2011 revisions to DIBP's MDS mean that some alerts identified as deficient by Wheen testing standards are considered acceptable by DIBP's current standards.

3.30 As shown in Table 3.2, the percentage of data deficient records of all types has declined in the three years since testing was last undertaken in 2008. While data quality has improved, the improvements are qualified to some extent, given that the Wheen criteria only examined the completion of data fields, and not the content within the field. For example, entries such as 'unknown' are considered to be complete according to the Wheen criteria.

Table 3.2: Data deficient PAL records over time

	2003 (percentage)	2008 (percentage)	2012 (percentage)
Data deficient PAL records	9.3	19.9	2.2
Data deficient high risk PAL records	16.0	27.4	3.3
Data deficient records[1]	8.1	10.2	3.9

Source: ANAO Audit Report No.35, *Management of the Movement Alert List*, p. 57 and ANAO analysis of the MAL database as provided by DIBP.

Note 1: excludes national security records

Current CMAL data quality and MDS

3.31 The ANAO also considered DIBP's application of its MDS and compliance with the business rules for each ARC. Table 3.3 describes MDS compliance by ARC with both mandatory and desirable standards.

3.32 Analysis shows that compliance with the MDS is highly variable by ARC.[71] Those ARCs that show higher levels of MDS compliance typically comprise records of individuals for whom DIBP has information already available from other immigration systems, that is the immigration specific alerts such as ARCs 10, 11, 12, 14 and 16. ARC07 alerts are frequently added as a result of individuals identified at border entry or at the initial visa application stage, in which case, there is normally substantial information available to the officer adding the alert. Alerts with lower compliance, such as ARC03 (war crimes), will have lower MDS compliance as listings are generally received from external parties and typically contain less information. As noted earlier, DIBP accepts a lower level of compliance for high-risk alerts, given the sensitivity of the listing and consequences of a missed match.

3.33 The ARC with the lowest MDS compliance, ARC25 (serious criminal poor biodata) was specifically created to store alerts for individuals for whom very little information is available. The issue for DIBP's consideration in relation to ARC25 records is whether it is viable to maintain an alert category for which so little information is available that maintaining the ARC is neither effective nor efficient.

[71] The variation is to be expected, given the different MDS which apply to each ARC and the variability in data quality that results from alerts in the high risk categories.

Table 3.3: Proportion of records meeting 2011 minimum data standards

Alert Reason Code (ARC)	Percentage of total records		Meets mandatory requirements		Meets desirable requirements[1]	
	Number of records	Percentage of records	Number of records	Percentage of records	Number of records	Percentage of records
ARC03	7 997	1.6	3 366	42.1	2 408	30.1
ARC04	4 723	0.9	3 254	68.9	1 873	39.7
ARC05	128 559	25.2	126 315	98.3	110 090	85.6
ARC06	81 990	16.0	78 816	96.1	N/A	
ARC07	17 555	3.4	17 361	98.9	16 573	94.4
ARC08	2 915	0.6	2 727	93.6	N/A	
ARC09	63 715	12.5	59 048	92.7	N/A	
ARC10	43 290	8.5	36 425	84.1	N/A	
ARC11	19 174	3.8	17 291	90.2	N/A	
ARC12	80 343	15.7	74 482	92.7	N/A	
ARC13	14 732	2.9	12 017	81.6	N/A	
ARC14	16 530	3.2	15 201	92.0	N/A	
ARC16	16 821	3.3	15 020	89.3	N/A	
ARC17[2]	1	0.0	1	100.0	N/A	
ARC18	8 073	1.6	5 043	62.5	2 700	33.4
ARC19	624	0.1	397	63.6	396	63.5
ARC20	3 310	0.6	3 182	96.1	3 182	96.1
ARC25	783	0.2	65	8.3	45	5.7

Source: ANAO analysis of CMAL database as provided by DIBP.

Note 1: ARCs marked ‘N/A’ do not have desirable requirements.

Note 2: At the time of audit, MAL contained one ARC17 record. This figure has been rounded down to 0.00%.

3.34 Levels of compliance with desirable MDS criteria are lower than for mandatory criteria. Desirable criteria provide additional information to assist CMAL and the BOC in making a match decision. Only ARC20 (skilled migration fraud) alert records attained equal levels of compliance with both mandatory and desirable criteria. However, overall, rates of compliance with the desirable criteria are increasing.

Quality of CMAL database records since September 2011

3.35 The quality of CMAL records has improved over time, particularly since the introduction of the latest MDS in September 2011. The 98 121 (20 per cent) records held in CMAL that have been created in the period September 2011 to November 2012, exhibit a higher degree of MDS compliance.[72] Table 3.4 shows that, of the 413 014 records listed on the database pre-September 2011, over 90 per cent meet mandatory requirements and almost 80 per cent meet the desirable requirements. Of the 98 121 records created since September 2011, 99.7 per cent meet the mandatory requirements and 88.6 per cent meet the desirable requirements.

Table 3.4: Records meeting September 2011 MDS

Time period	Percentage of total records in time period		Meets mandatory requirements		Meets desirable requirements	
	Number of records	Percentage	Number of records	Percentage	Number of records	Percentage
Records listed pre-September 2011	413 014	80.8	372 140	90.1	117 374	78.7
Records listed post-September 2011–November 2012	98 121	19.2	97 871	99.7	19 893	88.6

Source: ANAO analysis of CMAL as provided by DIBP.

3.36 The CMAL database still contains approximately 41 124 non-compliant records (8.05 per cent)[73], which will continue to affect data matching capability. One of the challenges faced by DIBP is the extent to which resources can be devoted to the review of the relatively small number of legacy alert holdings when current match resolution queues remain (see paragraphs 4.24–4.30). DIBP advises that, as time goes by, legacy alert holdings will expire, and their impact will progressively reduce. However, as noted above, expiry periods are generally lengthy: seven of the 19 ARC categories have expiry dates of

[72] PAL records minus national security records.

[73] PAL records minus national security records.

three years from their creation, one at age 18 and the rest have expiry dates of 100 or 120 years of age or 100 years from creation. Consequently, it will take many decades for the legacy holdings to work through the system.

DIBP's standards for complete records

3.37 The MDS vary in the extent to which a record is considered complete, given that for some data fields 'unknown' or '-' are acceptable as valid entries. However, '-' and 'unknown' type entries are sometimes used in non-name fields, and surname fields. If the 86 509 'unknown' type entries[74] are not considered as meeting the requirements of the MDS, MDS compliance rates fall. Table 3.5 below shows the MDS compliance of CMAL records when unknown-type entries are acceptable, and when unknown-type entries are excluded.[75]

Table 3.5: Records meeting September 2011 MDS (all entries; 'unknown' type entries excluded)

	Meets Mandatory Requirements		Meets Desirable Requirements	
	Number	Percentage	Number	Percentage
Completion Acceptable – all entries	470 011	91.9	137 267	80.0
Completion acceptable - 'Unknown'-type entries excluded	383 502	75.0	116 062	67.6

Source: ANAO analysis of CMAL as provided by DIBP.

3.38 CMAL's post-September 2011 records, that is those created following the introduction of revised MDS, still exhibit an improved level of data quality, even allowing for the exclusion of unknown-type entries. Table 3.6 outlines the proportion of records for each time period that comply with mandatory and desirable MDS requirements, excluding unknown-type entries as completed fields. DIBP's use of these entries in CMAL alerts has reduced over time.

[74] The ANAO considered as 'unknown-type' entries name fields that contained only '-', date fields of '0', genders of 'Unknown' and 'Not Stated', countries of birth of 'UNKN' and citizenships of 'XXX'. Note, this figure captures only the records with 'unknown' type entries that do not meet the mandatory requirements; not all records have desirable requirements and there is overlap between mandatory and desirable.

[75] ANAO analysis counts "-" in the first name field as a valid entry if the MDS for that ARC explicitly states that is acceptable, as it does for ARCs 06, 08 to 17, and 19.

Table 3.6: Records meeting September 2011 MDS ('Unknown' type entries excluded; records created pre and post September 2011)

Time period	Percentage of total records		Meets mandatory requirements		Meets desirable requirements	
	Number	Percentage	Number	Percentage	Number	Percentage
Pre-September 2011	413 014	80.8	297 312	72.0	97 763	65.5
Post-September 2011	98 121	19.2	86 190	87.8	18 299	81.5

Source: ANAO analysis of MAL database as provided by DIBP.

Conclusion

3.39 The ANAO's analysis of the CMAL database indicates improvement in the quality of the data currently held in CMAL. The 2010 strategies to improve CMAL data quality, through the revised MDS and centralised control over data entry within the BOC have been broadly effective. However, the ANAO notes that the MDS are not rigorously enforced, with 8.05 per cent (41 124) of records not meeting mandatory requirements.

3.40 In the absence of an effective review mechanism, the quality of the 80 per cent of records created prior to 2011 will not improve until these records expire, which in most cases will not be for many decades. The ANAO recognises that enforcement of MDS carries with it a risk of an administrative overhead. However, alert records with poor quality data can compromise CMAL's matching capability, and data deficient alerts are also less likely to be useful to visa and citizenship decision makers. The implementation of an effective review strategy as proposed in Recommendation 3 (paragraph 3.25) should minimise the impact of data deficient alerts in CMAL.

4. Measuring and Reporting CMAL Performance

This chapter assesses the processes DIBP has in place to monitor and report on CMAL's performance.

Introduction

4.1 As previously noted, CMAL has an important role in Australia's border security and immigration processing arrangements. It is therefore important that DIBP is able to demonstrate the effectiveness of CMAL operations and supporting administrative arrangements. As noted in the 2008 audit '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'.[76]

4.2 The 2008 audit found that DIBP's performance reporting capability was limited, that there was a lack of information to demonstrate how successful or otherwise MAL was at achieving its objectives and the ability to detect system failures within an appropriate timeframe was limited.[77] These findings echoed those of successive reviews of the MAL database over the previous decade, particularly the Wheen and Gerlach[78] reviews, both of which recommended substantial additional reporting of performance information.[79] The ANAO made three recommendations to address these shortcomings, covering performance reporting (Recommendation No. 3), management information (Recommendation No. 4) and quality assurance measures (Recommendation No. 5).

4.3 In order to assess DIBP's progress in improving its performance reporting, management information and quality assurance measures the ANAO examined:

- DIBP's approach to performance reporting, including an analysis of current reporting arrangements;

[76] ANAO, Audit Report No. 35, 2008–09, op cit, p.118.

[77] Ibid, pp. 17–18.

[78] DIBP, internal review of MAL Technical/Operation Review, April 2000, (the Gerlach Review).

[79] ANAO, Audit Report No. 35, 2008–09, op cit, p.128.

- the management information collected and available to CMAL managers; and
- DIBP systems quality assurance arrangements.

CMAL performance reporting

4.4 The 2008 ANAO report found that DIBP produced no data to demonstrate the effectiveness of MAL in the context of the visa and citizenship application process and that DIBP could not demonstrate how successful MAL was in achieving its outcomes. The audit report suggested that performance information could include data on DIBP'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 obtaining Australian citizenship.[80]

ANAO Report No.35 2008–09: Recommendation 3

The ANAO recommends that DIAC improve its reporting on the performance of MAL by, where practicable, identifying instances where MAL has alerted decision makers to information that has been the reason, or part of the reason for decisions on visa and citizenship applications.[81]

4.5 In agreeing to the ANAO's recommendation, DIBP advised that, with the advent of CMAL, it intended to regularly sample 'true matches and track through the decision making process to determine what role MAL information has played in the visa decision'.[82] One of the difficulties confronting DIBP in developing accurate reporting of CMAL's impact on decision making is that there is no compulsion or requirement for a visa processing officer to include the reason for a decision or information about the basis for a decision in the decision record.

4.6 In 2010, consistent with its response to the ANAO, DIBP funded a project to measure CMAL outcomes (and to consider the strategic development of CMAL). Part of the project included developing business information through the manual analysis of a number of visa grant decisions

[80] Ibid, pp 17-18.

[81] Ibid, p.127.

[82] Ibid, p.127.

where the decision record was reviewed with the visa processing team. Some of the key findings of this analysis were:

- in 2009–10, 2.97 million Match Identifier/PAL combinations were assessed against ARC05 serious criminal alerts, resulting in over 4 000 true match decisions;
- from November 2008, 5 915 identities were true matched against ARC05 alerts and this information was available to visa and citizenship decision makers. The decision maker chose to override the red[83] CMAL status for ARC05 cases in only 8 per cent of true match cases.

4.7 In addition, a report to the Executive Committee of DIBP in November 2010, set out the following findings:

- between November 2008 and October 2010, 201 532 individual clients had been true matched to an alert;
- of these 201 532 clients, in 78 per cent of cases, the delegate directly considered the advice provided, choosing not to seek an override and declining the citizenship or visa outcome;
- in 45 012, or 22 per cent of cases, the delegate considered the information provided and chose to override the red status and continue the visa or citizenship application process.

4.8 The evaluation of CMAL's impact on outcomes undertaken in 2010 proved useful to DIBP. The results were used to inform the department's response to the JCPAA in October 2010, a high level strategic paper to the DIBP Executive Committee in November 2010, and a submission to the ANAO following commencement of this audit in February 2013. DIBP has not, however, undertaken further evaluations to measure CMAL outcomes, as the ANAO recommendation intended, citing the time and resource intensive nature of the exercise, although DIBP has not provided details of the costs involved.[84] In order to build on this baseline data, the ANAO considers that

[83] A red CMAL status is a status assigned to a client who has been assessed as a true match against the CMAL database.

[84] DIBP considers that demonstrating the effectiveness of CMAL is complex because CMAL data comprises only part of the information available to the Minister's delegate when making a decision on a visa or citizenship application. This can make it difficult to isolate the influence of CMAL data on individual decisions. Further, the exercise was a manual one, undertaken over several months and with several officers involved at various stages. The evaluation was not costed at the time and DIBP considers that it would be difficult to develop an accurate costing now.

there would be benefit in investigating stream-lined and cost effective options for periodically duplicating, potentially on a sample basis, the earlier exercise to enable data performance comparisons over time as well as measure CMAL's contribution to Australia's border security efforts. This information would assist DIBP to better advise the Parliament and also provide a basis for more informed decision making in relation to CMAL.

Measuring data matching effectiveness

4.9 In the absence of performance information on the impact of CMAL in the context of the visa and citizenship applications, DIBP has sought to assess the performance of CMAL more narrowly: in terms of the system's effectiveness in matching data. DIBP advised the ANAO it uses two measures for this purpose:

> The first is ensuring that all DIBP clients are checked against CMAL ... The second key performance measure is our ability to accurately match clients.

4.10 The visa and citizenship systems require DIBP decision makers to consider a client's CMAL status prior to making a decision on a visa or citizenship application. It is a system enforced inquiry whereby the decision maker cannot proceed to the next step unless CMAL has been checked. If the system returns a 'green' CMAL status then no further action is required from the decision maker, who can then proceed with processing the application. However, if a red status is returned, either the decision maker or the BOC must provide an override code for the visa or citizenship application to proceed further. If an amber status is returned only the BOC can provide an override code.

4.11 The requirement to check CMAL before proceeding with a visa or citizenship application raises a question of law. The 2008 audit report noted that DIBP did not have the capacity to *require* delegates to check CMAL prior to making a decision on a visa or citizenship application and that the current DIBP process could restrict the decision maker's discretion, which, in legal terms, is absolute.[85]

4.12 DIBP has put in place administrative directions to require delegates to check the narrative in CMAL prior to making a decision on visa and

[85] ANAO, Report No. 35, 2008-09, op cit, p.111.

citizenship applications. However, no corresponding legislative change or ministerial direction under s 499 of the Migration Act has been sought by the department. It would be prudent for DIBP to seek assurance that current procedures are lawful, and if there is any doubt, to identify the appropriate legal remedy.

4.13 In the CMAL context, DIBP's reporting and monitoring has centred around detecting and rectifying mistakes, such as missing a true match, particularly in the case of national security records, as well as managing match case volumes, (the amber queues are discussed at paragraphs 4.26–4.31).

4.14 DIBP undertakes individual assessments of missed matches. Nine missed matches were identified in the period January 2010 until February 2011, all of which were national security alerts. No further missed matches were identified in the period from February 2011 to October 2013.[86] All missed matches were assessed by the Assistant Secretary Border Operations Branch and a minute was forwarded to the DIBP Secretary advising of the missed match and the outcome of the review process. All missed matches related to visa applicants prior to arrival and were the result of human error. The department advised that at no time did any of the missed matches result in persons being admitted to Australia when they should not have been.

4.15 DIBP also provides the following match case data in its monthly statistical report:

- incoming, completed and cancelled match cases;
- the breakdown of completed match cases between the BOC and the system;
- the count of true matches by ARC and by score; and
- the count of non-matches by ARC and by score.

4.16 Since the 2008 audit, DIBP has implemented systems improvements aimed at increasing matching accuracy and harmonising matching rules across government. DIBP anticipates that using similar rules will improve matching accuracy, and reduce the number of false matches referred for resolution.

[86] An additional missed match was detected in early November 2013.

The Business Intelligence Platform (Data Warehouse)

4.17 DIBP has regularly advised that it was enhancing CMAL performance reporting through its Business Intelligence Platform (Data Warehouse).[87] In 2009, DIBP advised the Joint Committee of Public Accounts and Audit (JCPAA) in response to a question on notice[88] that:

> DIAC is developing a range of reporting tools that will be able to interrogate the data held in the Business Intelligence Warehouse. The CMAL data is scheduled to be integrated into the new warehouse by June 2010. This will provide a range of routine reports and the mechanism for creating ad-hoc reports to cater for the range of queries with respect to data quality to assist the Border Operations Branch staff and key data owner stakeholder (*sic*) to better identify areas of vulnerability.

4.18 In February 2013, DIBP advised the ANAO that 'CMAL performance reporting will continue to mature as DIBP's data warehouse reporting capability is further enhanced'. DIBP has more recently advised that performance reporting out of the business intelligence data platform is a three stage process; incorporation of data from the source, integration of the data with all other data in the warehouse and ultimately development of the reporting capability. To date, only stage one, incorporation of the data, has been effected. The remaining stages are awaiting approval.

4.19 The performance reporting capability for CMAL, potentially available through the data warehouse, is now more than three years overdue and until that capability is fully developed, the department's performance reporting options for CMAL are severely restricted.

Conclusion

4.20 In summary, DIBP still collects no performance information routinely on the impact of CMAL on visa and citizenship application decisions. DIBP's current focus on the effectiveness of the system's matching capability may

[87] The Business Intelligence Platform (BIP) is a business intelligence system. In broad terms, the BIP is a data warehouse environment with the associated infrastructure and tools to facilitate the integration of data for management reporting. In simple terms, the BIP is a reproduction of DIBP operational data that is specifically stored for reporting, querying and analysis. The Business Intelligence Platform (BIP) extracts and transforms information from a myriad of discrete departmental systems, storing the information in the one place, presenting information in a common and easily accessible format and making the information available for reporting.

[88] The question on notice was: 'What steps has DIBP taken to improve the measurement of, and reporting on data quality, MAL reliability and client service?'

provide insight into the accuracy of data matching and assurance around missed matches, but provides only a limited view of CMAL's performance and utility. While Recommendation No. 3 has not been effectively implemented, DIBP has commenced the process of integrating CMAL data into its business intelligence warehouse, prior to the development of a reporting capability. Completion of this project will enable DIBP to deliver targeted performance information.

Recommendation No.4

4.21 To better demonstrate CMAL's contribution to Australia's border security arrangements, the ANAO recommends that the Department of Immigration and Border Protection investigates cost effective options for periodically identifying and reporting on those instances where CMAL data has been influential in visa and citizenship decisions.

Agency response

4.22 *Agreed. DIBP will continue to work to improve the availability and scope of CMAL reporting.*

CMAL management information

4.23 The 2008 audit concluded that management information on MAL was limited and that there were opportunities for improved management reporting relating to the data quality of new entries, client service standards and overall system reliability. The ANAO made the following recommendation:

ANAO Report No.35 2008–09: Recommendation 4

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

- data quality;
- MAL's reliability; and
- client service, measured by the service level agreements agreed internally with CMAL client areas of the department.

4.24 In February 2013, DIBP advised that, in respect of the previous audit's Recommendation No. 4, 'comprehensive systems and service levels' have now been put in place. These include:

- the implementation of a service level agreement (SLA) which commits to internal service level standards for the amber queues[89]; and
- reporting produced by the Data Management and Reporting Team.

4.25 The ANAO examined these arrangements, and also considered alternative sources of management information.

The amber service level agreement and match queues

4.26 The SLA commits the BOC to providing a response to the relevant visa processing system within an agreed timeframe for each category of applicant. All match cases are placed in a queue, which is addressed by a BOC officer according to the priority accorded the queue number. Generally, the lower the queue number, the less urgent the situation and the lower the priority for resolution. CMAL priority queues nine through to three are made up of 'pre-visa grant' potential match cases and are prioritised by the system according to visa type as agreed with the service delivery network (SDN). For example, the priority 10 queue, contains clients at a border location and urgent case escalations and has a resolution time of less than 60 minutes. In contrast, the priority three queue, with a resolution time of 15 days, contains applicants for permanent entry, citizenship or New Zealand passport holders. Match case analysts in the BOC assess potential matches for those clients with an amber status, based on the CMAL priority. The agreed standard for resolution of a queue is resolving a minimum of 85 per cent of cases within the agreed timeframe.

4.27 It is also possible for BOC staff to manually select cases from specific queues for resolution. The CMAL priority two queue is a maintenance queue, containing post visa grant clients, whose CMAL status has changed to amber (meaning a potential match case). This status change is due to either a change in biodata or to a new alert being added to the system that has triggered a potential match against the client. The BOC has an agreed SLA with the SDN of two days to resolve the match cases in this queue.

4.28 The priority one queue (the lowest priority) is made up of potential match cases with no context information, meaning a visa type has not been entered into the visa system. Match analysts do not process match cases in this

[89] The amber queues (1-10) consist of clients with a CMAL status of amber; they either have not yet been assessed against CMAL or are a potential match to an alert and are awaiting match case resolution.

queue and there is no timeframe specified for resolving this queue in the SLA. When, and if, context information becomes available the match cases are automatically moved into their correct priority queue.

4.29 Match cases dynamically move between queues and CMAL automatically prioritises a client according to the events occurring along the travel pathway.[90] A client at the border will be automatically moved into the priority 10 queue as necessary. There is therefore minimal business risk from a match case in a low priority queue exceeding its SLA, as time-critical events such as check-in will automatically prioritise the case.

4.30 The BOC receives snapshot reports on a daily basis that provide information about those cases that will potentially breach or have breached the SLA. For each service level queue the report shows the number of open, assigned, referred and total cases as well as the numbers breaching the SLA timeframes. This report is used to assess the status of each of the queues and the workflow within the BOC. For example, the report for 0733 hours on 14 December 2012 shows the two and three queues, which have resolution times of 48 hours and 15 days respectively, being responsible for almost 100 per cent of the SLA breaches. Only five SLA breaches are shown for the 10 queue and two for the nine queue.

4.31 DIBP advised that it is considering amendments to the daily snapshot report. Because the queues are dynamic, the daily snapshot report is not satisfactory as a management tool; it is a point in time report when a real time report would be more useful. The Borders Operations Branch is working to develop more useful reporting options, including the development of a real time report of match cases reaching their SLA standards in each queue.

Data management and reporting

4.32 A Data Management and Reporting Team (DMRT), located within the BOSS, generates a suite of reports for the CMAL environment. The CMAL report catalogue comprises over 100 reports, including 19 regular monthly reports, three produced weekly and one daily report. The remainder (almost 80 reports) are the result of ad hoc requests and the DMRT retains the report request. Many of the reports focus on the statistical analysis of CMAL activity, while others provide details of Australians on the database. Some reports

[90] Discussed at paragraphs 1.10-1.12 in Chapter 1.

address data quality issues and provide management information about performance.

4.33 The primary CMAL management report produced by the DMRT is the monthly CMAL management report (CMAL statistics). This report provides:

- PAL and DAL holdings;
- the number of referrals to ARC owners for resolution; and
- incoming and completed match case information for a rolling three month period.

4.34 This management report is useful for an overarching picture of CMAL holdings and BOC activity and is used by the Border Operations Branch to identify trends in holdings by ARC, DAL holdings, and match case data and performance.

4.35 The CMAL system and the DMRT have the capability to produce a wider range of reports on a regular basis to assist the Branch and the ARC owners to manage data holdings more effectively. For example, the DMRT produced a draft stakeholder report for ARC08 (child custody concerns) in April 2013. The report provided a snapshot of ARC08 holdings against total CMAL data holdings, ARC08 match cases and true matches and also identified data quality issues with active ARCs. This report enabled the ARC owner to identify how many records were data deficient and where the MDS were being breached, all of which is information which will assist in review of data holdings. DIBP advised that the idea of ARC stakeholder reports was raised at the first AOCF by the DMRT but due to the lack of CMAL knowledge on the part of ARC stakeholders, further production of such reports was delayed until after CMAL information sessions were delivered.

Other management information options

4.36 DIBP's management reporting primarily focuses on the production of statistics and reports on the management of the CMAL queues. However, there is potential for DIBP to collect information on aspects of CMAL support operations, including information:

- that will assist in the identification of alerts with poor data quality;
- about the effectiveness of certain administrative processes supporting CMAL; and
- about the utility of some alert categories and holdings.

4.37 DIBP could also undertake analysis of discrete parts of the CMAL system such as the narrative element of the alert record, the BOC's oversight of alerts proposed through the RIF, and the profile of ARC override activity.

Alert narratives as an analytical tool

4.38 Both the PAL and DAL alert records contain narratives, which are free text fields that provide essential background information and a chronological history of the alert record. A good narrative will contain clear and unambiguous information that will assist in the resolution of a true match. Because narratives are essential in providing context to the alert, high quality narratives assist in raising the quality of alert records and their usefulness to DIBP staff in deciding a true match.

4.39 The CMAL PAM3 imposes few mandatory requirements on narratives, but they must contain, at a minimum, a brief overview as to why the person or document is listed on CMAL, instructions detailing the actions border staff should take if they encounter the person or document, and references to any files or documents that may contain additional information. Narratives should not contain information based on subjective considerations, such as personal opinions.

4.40 In the context of the review of narratives and the training provided to staff in the writing of narratives, DIBP advised:

> As part of the RIF process, and as part of the monthly error report, a comprehensive review of the narratives held in a record is performed. As a quality assurance measure all proposed additions and amendments are reviewed before being listed on the PAL or DAL. To adhere to the standards, specified in CMAL PAM3 titled 'Listing Identities or Documents on MAL', the entire alert is reviewed to ensure it meets the general requirements of listing. An e-learning package on the CMAL RIF is available to all DIBP staff. This training package provides guidance to staff on what should be included within a narrative.

4.41 As noted in paragraphs 3.11 and 3.12, DIBP relies on the initial BOC review of proposed CMAL alerts and amendments through the RIF to provide quality assurance, including for the narratives. Further, the monthly error report produced by the DMRT does not review the PAL narratives and DAL alerts are limited to major errors such as the omission of the permissions requirement for Australian citizens in the narrative.

4.42 The ANAO examined the CMAL RIF e-learning training package to assess its utility in terms of the narrative requirements set out in the CMAL PAM3 and also assessed the quality of a limited range of narratives.

E-learning training package

4.43 The CMAL RIF e-learning training package contains three modules, proposing a new alert, expiring an alert and amending a narrative. The modules are simple and the instructions relating specifically to the narrative refer to the 'existing standards that you have' or 'existing business rules'. There is no detailed information available to the trainee in the e-learning package on either the quality or the type of information to be provided in the narrative. The e-learning package therefore has limited utility in improving the quality of narratives.

ANAO analysis of narrative data and requirements

4.44 To assess the quality of narratives the ANAO examined its copy of CMAL, focusing on two kinds of entries: the narratives for Australian records, for which there are precise requirements set out in the CMAL PAM3; and narratives containing information, which should have led to the expiry of the alert record but where the alert record remains on the database.

4.45 Listing of Australians on CMAL is subject to strict controls. One of the requirements set out in the CMAL PAM3 is that the narrative contain a paragraph about the consent requirement before an Australian citizen can be detained or questioned at the border.[91] Of the 182 persons with Australian citizenship listed on CMAL, 141 (77 per cent) do not have a narrative containing phrases that indicate the presence of the consent requirement.[92]

4.46 There are also a number of narrative phrases that suggest that an expiry of the record would be appropriate. These phrases include 'request delete', 'client is deceased'[93] and 'cancellation of an Interpol notice'. ANAO analysis found:

[91] There are no powers under the *Migration Act 1958* that allow DIBP officers to detain and question Australian citizens in immigration clearance once a person has satisfied an immigration officer that they are an Australian citizen. Therefore, DIBP officers must ask for and receive the consent of the Australian citizen to detain that person for further questioning beyond clarification of identity.

[92] The figures cited in this paragraph are derived from the copy of the CMAL database provided to the ANAO in November, 2012.

[93] DIBP advises that while a person is deceased, the identity may still be used for travel purposes. For this reason names of deceased persons can still appear in the database.

- approximately 200 narratives that appear to request deletion;
- some narratives for clients who were obviously deceased and whose identity is an unlikely one to be assumed, including one individual from the US Marshall's list identified in the previous ANAO audit who remains on the database; and
- approximately 2 000 narratives mentioning cancelled Interpol notices.[94]

4.47 The significance of the narrative to the match function, the high proportion of legacy holdings with relatively poor narratives and the necessity to ensure new alerts are compliant, merits ongoing evaluation of the narrative entries. This will promote data quality and provide management information on the trends in data quality. It would be beneficial for DIBP to examine the quality of proposed alerts to provide data about the extent to which the narrative contributes to the accuracy of the match resolution process.

4.48 DIBP could assess the quality of the proposed alerts and the narrative by analysing on a regular basis (for example annually):

- approved and rejected alerts to assess whether they were appropriately approved or rejected, that is:
  - whether approved alerts conform to the MDS for each ARC and whether rejected alerts were appropriately rejected; and
  - the number of data deficient alerts knowingly accepted by the BOC and the reasons why;
- the content of the narratives of proposed alerts that are returned to the proposer for additional information to determine where the deficiencies lie; and
- the content of the narratives in proposed alerts that are accepted by the BOC to determine if alerts are data deficient without a business case supporting the listing.

4.49 It would be worthwhile to undertake this quality assurance exercise retrospectively and without notification. It could be repeated at periodic intervals and would provide trend data, assurance of BOC processes and compliance by DIBP staff in the network with the CMAL PAM3 standards.

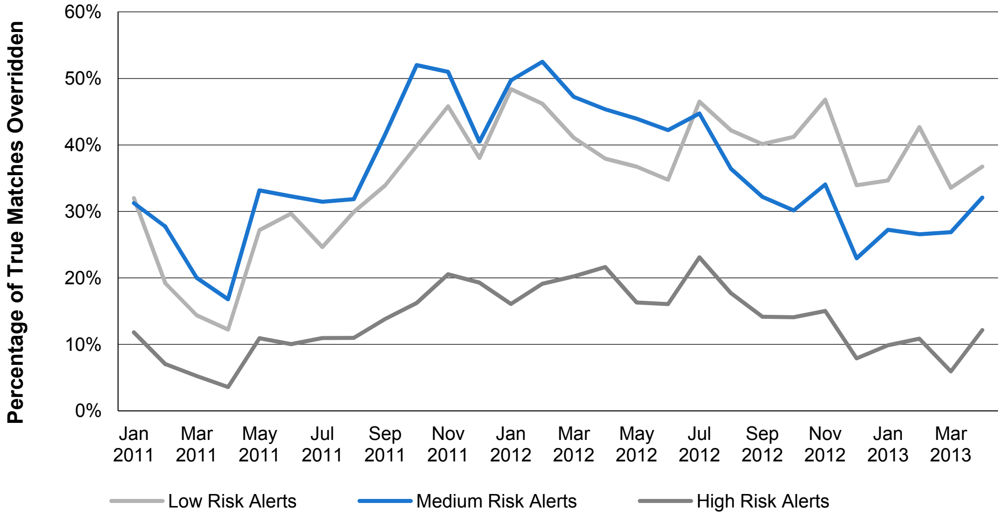
[94] Interpol Notices are discussed in Chapter 5.

Analysis of override data for database management purposes

4.50 CMAL is able to record the reasons for an 'override', which is recorded where there is a true match and the decision maker, having considered the CMAL information, decides that the visa or citizenship application should continue to be considered, or a visa issued or citizenship granted. Analysis of the override reports provides information on which alert records are most frequently overridden and why. This information is potentially useful for ARC owners in their management of data holdings, and to the Borders Operations Branch to assess the utility of particular ARCs and to understand the reasons for the overrides.

4.51 The ANAO requested override data for the calendar years 2011, 2012 and year to date (2013) by ARC alert holdings. From the beginning of 2011 to March 2013, a total of 107 257 alerts were overridden (approximately 48 000 overrides per annum). Figure 4.1 shows the rate at which low, medium and high risk alerts were overridden during this period.

Figure 4.1: Percentage of true matches overridden by ARC risk category

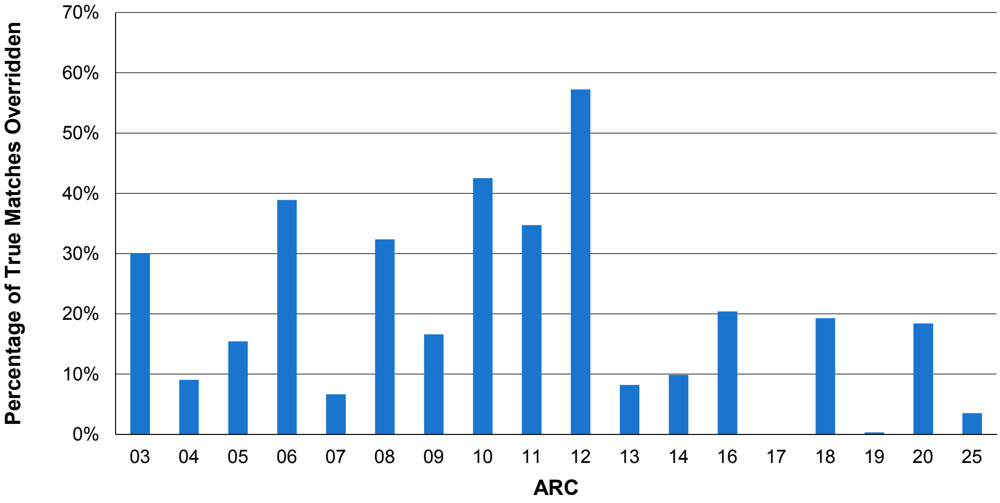


Source: ANAO analysis of CMAL reporting.

4.52 High risk match decisions are overridden infrequently, (between 10 and 20 per cent of the time), whilst medium and low risk match decisions have historically been overridden as often as 50 per cent of the time (ARC12, debts to the commonwealth in particular). Low and medium risk alerts are disproportionately represented in override statistics, given their contribution to total match decisions. Over the period January 2011 to March 2013, 58 per cent of overrides resulted from low-risk alerts, despite this category of alerts making up only 22 per cent of CMAL alert holdings. High risk alerts, 62 per cent of the CMAL database, generated only three per cent of total overrides during that period. Thirty three per cent of overrides were for medium risk alerts (16 per cent of the CMAL database) with the remaining six per cent of overrides resulting from DAL alerts.

4.53 An ARC with a high rate of overridden decisions may suggest that the value of the ARC is low. These ARCs create considerable administrative workload for DIBP without having a significant impact on visa grant/entry outcomes. Figure 4.2 shows the percentage of true matches overridden for each ARC in the time period for which data is available.

Figure 4.2: Percentage of true matches overridden by ARC, 2011–2013



Source: ANAO analysis of CMAL reporting.

4.54 As indicated above, the low risk ARC10 (overstayers) and ARC12 (debts to the Commonwealth) are most frequently overridden. By contrast, higher risk alerts such as ARC05, despite generating a greater volume of potential matches, are more likely to lead to a true match that is not overridden by the decision maker.

4.55 DIBP does not routinely analyse the overrides for information about the reasons for an override or the instance of overrides by ARC. This type of analysis of has considerable value in managing the ARC system, particularly in relation to the extent to which individual ARCs have a bearing on visa and citizenship applications. For example, if a particular ARC is never or rarely a factor in the granting of a visa or citizenship application, that is the alert is overridden consistently, the inclusion in the CMAL database of alerts attached to those ARCs or the ARC itself might be an issue for consideration by DIBP.

4.56 In response to the ANAO's analysis, DIBP advised that it will be pursuing further analysis around CMAL outcomes and performance, once its data refresh exercise is completed and 'stability returns to the CMAL processing workload'. The ANAO notes that, as a visa grant is the subject of separate quality assurance processes, it may be possible for DIBP to build into their visa quality assurance processes some CMAL performance data which can be accessed by the Border Operations Branch.

Conclusion

4.57 DIBP produces some useful management information but often on an ad hoc basis, in part due to capacity constraints. There is the capability within CMAL for DIBP to improve the scope of the management information produced. In particular, analysis of alert narratives, override data and the quality of proposed alerts has the potential to provide DIBP with management information which could enhance the operation of the CMAL system. DIBP has not focused sufficiently on this type of management information to date. There may also be potential for the visa processing quality assurance processes to incorporate some CMAL performance data to enhance DIBP's CMAL performance reporting.

Systems quality assurance processes

4.58 DIBP, as manager of CMAL, must assure itself and its stakeholders that the systems underpinning CMAL are working satisfactorily. Furthermore, as Customs has responsibility for the primary immigration clearance function on behalf of DIBP, both agencies require assurance that their systems support the efficient clearing of travellers and that any problems are communicated and dealt with in a timely manner. The 2008 audit noted that, at times, parts of MAL had failed, the systems failures went undetected and these failures had remained undetected for an extended period.[95] The report recommended that

[95] ANAO, Audit Report No. 35, 2008–09, op cit, p.18.

DIBP seek to measure and report on MAL's reliability[96], and also made the following recommendation.

ANAO Report No.35 2008–09: Recommendation No. 5

The ANAO recommends that DIAC implements a mechanism for providing regular assurance that all key parts of the MAL system are operating satisfactorily.[97]

4.59 DIBP has responded to this recommendation by implementing a number of mechanisms to address systems performance issues, including:

- developing memoranda of understanding with key external stakeholders;
- introducing CMAL application performance reports, which detail:
  - response times for the CMAL system against service level agreements;
  - increases/decreases in user numbers and transaction volumes including checks on the outcomes of surges in demand; and
  - instances of downtime and length of time of each occurrence; and
- taking specific actions to address system failures identified in the previous audit report.

Reporting requirements under the Memorandum of Understanding with Customs

4.60 The MOU between DIBP and Customs provides the framework for managing their information technology systems and promotes a nationally consistent approach to their working relationship. The document provides for systems availability notifications, communications, systems performance standards and business continuity planning.

4.61 The IT Annex requires reports for system availability, system performance and system auditability. All but one of these reports is produced

[96] Ibid, pp. 127 and 136.

[97] Ibid, p. 137.

by Customs. The reports are provided to the Passenger Business Systems Working Group (PBSWG)[98] for consideration at its monthly meetings.

4.62 DIBP has developed a definitions document to specify more precisely the parameters for reporting under the IT Annex. The document was developed following the identification by DIBP of errors in initial reports from Customs. DIBP subsequently developed detailed specifications for the content of sub-sections within the Customs-DIBP MOU summary report. The document is currently being analysed by Customs, which will advise on whether Customs can meet the proposed requirements.

4.63 The IT Annex to the MOU was signed in 2010 and the definitions document was developed in December 2011, but to date no regular reporting corresponding with the terms of the annex has been developed to a stage where it is useful. DIBP advised the ANAO in September 2013 that both organisations are working together to resolve the issues:

> This work is ongoing and we met with Customs two weeks ago to discuss some reports they have and whether these would satisfy our requirements. Discussions between BOSS & Airports Policy on this are ongoing and all parties are committed to establishing regular and accurate reporting as outlined in the MOU.

4.64 DIBP advised that it is developing key performance indicators (KPIs) for the reports specified in the IT Annex but these are still in the early stages.

Reporting requirements under the Memorandum of Understanding with ASIO

4.65 The systems provisions in ASIO's MOU are less complex because there is limited systems interactions between CMAL and ASIO and there is no need to reconcile disparate copies of the database. DIBP provides a number of regular reports to the national security agency. These reports underpin the short and medium term approach to management of the national security holdings. Both agencies have a clear understanding of what the other agency will provide and on what basis.

[98] The PBSWG is the main Customs-DIBP forum established under the MOU IT Annex to discuss issues relating to information technology. The PBSWG meets monthly and its membership consists of Director level staff from DIBP and the Manager Passenger Enabling from Customs.

CMAL application performance reports

4.66 DIBP has developed an Application Monitoring and Reporting Plan, which sets out the parameters for the key applications performance report. The report is produced monthly and includes:

- response times and availability of key service delivery pages as detailed in the Application Monitoring and Reporting Plan; and
- user experience through Internet web pages.

4.67 The audience for this report includes the CMAL business and system owners, the Executive Production Control Authority, Production Systems Board, and Release Management. The report provides performance against key performance indicators (KPIs) for more than 40 types of transactions and identifies transactions within the KPI range and those breaching it. The report sets out observations on performance breaches with recommendations for actions to rectify any problems as well as the priority for these activities. User interaction with CMAL is reported on a daily basis, including identifying peaks and troughs in demand.

4.68 The application performance reports show that, generally, CMAL is reliable and responsive to users. The ANAO examined application performance data for the period January to June 2013, during which 33 of 41 metrics remained within established response targets for the entire six month period. One metric, the time taken to search for a person on PAL by a group identifier, remained outside targets for the entire period, however, this function is used infrequently.[99] Two other metrics, the time taken to retrieve a match case, and the time taken to search for a PAL record by biographic data, exceeded the 95th percentile targets for all six months, although average response times were within target during this period.

DIBP action to address systems failures identified by the MAL report

4.69 The 2008 audit report identified several specific system failures, including:

- corruption of the entry control point (ECP) MAL check;

[99] According to DIBP's June Application Performance Report, the group search function was used a total of 136 times between January and June 2013.

- failure to update the Customs copy of MAL; and
- failure to copy all MAL records when creating DIBP's 'MAL Contingency Database'.

DIBP considers that the implementation of the measures outlined below have resolved the systems problems identified.

MAL ECP checks

4.70 Under the HMAL system, MAL checks were manually performed by staff. While procedures required the check to be done, there was no enforcement by the system to ensure that this process was completed. Under the CMAL system, every individual entering Australia by air or sea, and every traveller applying for a visa or ETA, is checked for matches against CMAL alerts. It is not possible for a traveller or visa applicant to proceed to the next stage of entry or processing until their CMAL status is green, their amber status has been resolved or their red status has been overridden. DIBP considers that the ECP failure is no longer likely.

Customs' copy of MAL

4.71 In March 2009, DIBP advised the ANAO that the Customs copy of MAL had not been updated for a period of 13 months. DIBP discovered that the error in updating the Customs copy of the database in 2009 was not in HMAL itself, but in the process of extracting alerts. DIBP advised that the problem was resolved and to protect against further issues, DIBP and Customs now monitor the processing of alerts between CMAL and Customs Passenger Analysis, Clearance and Evaluation (PACE) system, with notifications to ensure staff are alerted if an update fails to complete successfully. DIPB advised that there has not been a recurrence of the problem since 2009.

The contingency database

4.72 The contingency database has similarly been overtaken by a systems improvement. Previously, MAL alerts were replicated to a MAL contingency database, to be used by the BOC in the event that the mainframe servicing HMAL was unavailable. In the 2008 audit report, an issue was identified where alerts from HMAL were not reliably replicated to the contingency database, which would have resulted in the database containing an incomplete set of records had DIBP needed to use it.[100] Additionally, MAL statistics generated for a period of time were incorrect, as the contingency database was the basis for MAL reporting.[101]

4.73 With the implementation of CMAL, HMAL has replaced the contingency database as the facility used by the BOC if CMAL is unavailable. DIBP has advised that the contingency database, while no longer used as a contingency, is updated every 30 minutes and used for quality purposes. The DMRT checks the contingency database for PAL and DAL errors each month and provides a report to the BOC.

Systems enhancements

4.74 CMAL software updates through the departmental wide Change Release system, take place three times per year in March, June and November. During the audit, for example, Change Release 08 took place on 22 March 2013, when DIBP upgraded its name matching software, together with several additional refinements.

CMAL disaster recovery

4.75 DIBP has developed disaster recovery plans for restoring the operation of CMAL in the event of an incident that interrupts its regular business operations. DIBP now has several plans that cover the transition of BOC staff and CMAL operations to an alternative standby site that may be used in a disaster. However, some elements of DIBP's CMAL documentation have not been updated to reflect current disaster recovery arrangements. The CMAL systems Data Management Plan includes information pertaining to the backup, recovery and testing of the CMAL database, but at the time of audit, these sections had not been completed.

Decommissioning of HMAL

4.76 The previous MAL database, referred to as Heritage MAL (or HMAL), has been retained for backup and ancillary purposes. Although DIBP originally envisaged decommissioning HMAL, it remains the primary interface between MAL and several other systems in the border security network. HMAL interacts with other systems such as:

[100] ANAO Audit Report No.35 2008–09, op cit, p. 134.

[101] Ibid, pp. 134–135.

- HMAL and TRIPS: ECP performs all PAL checks against HMAL, and TRIPS (via ECP) replicates all alerts in the HMAL PAL database to Customs for use in its own local copy of the PAL; and
- HMAL and ETAS: ETAS stores a local copy of the DAL for checking passport details at traveller check-in.

4.77 DIBP has confirmed that it still plans to decommission HMAL but no timetable has been established for the work.

Conclusion

4.78 The processes and systems enhancements that DIBP has put in place to ensure that that all key parts of CMAL are operating satisfactorily, have largely met the requirements of Recommendation No. 5 of the 2008 audit. The systems reforms and reporting measures implemented by DIBP mean that the deficiencies identified in the earlier audit are less likely to be repeated.

4.79 DIBP has in place detailed agreements with its external key stakeholders that address systems issues and quality assurance measures. The agreements provide for ongoing and regular reporting to keep both agencies informed about such matters as outages and impacts on passenger processing. However, DIBP and Customs have been slow to finalise development of the reports specified in their MOU. Although DIBP has advised the ANAO that current operational arrangements for systems assurance are effective, there would be benefits for both agencies in finalising the reports required under the IT Annex of the MOU.

5. Stakeholder Management

This chapter examines the arrangements that DIBP has put in place to deal with the major external stakeholders, who have a vested interest in CMAL.

Introduction

5.1 DIBP has a number of significant stakeholders who either undertake border security activity on its behalf, use CMAL data or who provide the data for inclusion on the CMAL database. The arrangements that DIBP has to manage these relationships are central to a successful border control strategy and the operation of CMAL.

5.2 As previously noted, the principal stakeholder agencies are Customs and ASIO. In addition, the Department of Foreign Affairs and Trade (DFAT) and the Australian Federal Police (AFP) are important stakeholders in CMAL as they provide data for inclusion on the CMAL database. While there are other agencies with an interest in CMAL, the consideration of stakeholder relationships has been limited to the principal external alert code owners, the AFP as a facilitator for DIBP access to Interpol systems for the listing of Interpol alerts and Customs as the principal service provider to DIBP.

5.3 The ANAO examined how DIBP manages its relationships with these agencies to promote effective CMAL operations and also to give those agencies an opportunity for input into the management of CMAL. The 2008 audit did not consider the relationship management aspect of MAL's operations.

The Australian Customs and Border Protection Service

5.4 The agency with primary responsibility for managing the security and integrity of Australia's borders is Customs. Customs' role is to provide effective border protection for the Australian community, whilst supporting legitimate trade and travel.[102] The relationship between DIBP and Customs is one of mutual dependence, particularly as CMAL is a key element in border control.

5.5 At airports and seaports, Customs undertakes the primary immigration clearance function on behalf of DIBP under the terms of the MOU agreed by

[102] Australian Customs and Border Protection Service, Annual Report 2011–12, p. xi.

the two agencies in June 2008 and the Annex to the MOU, *Immigration Clearance – Information Technology* signed in June 2010.

5.6 Under the terms of the MOU, data from several DIBP systems, including CMAL, is linked to Customs' Passenger Document Brokerage System, which in turn informs the Passenger Analysis, Clearance and Evaluation system (PACE). In the event that expected movement record (EMR) data is unavailable for a traveller, PACE checks the traveller's details against the Customs' HMAL copy of the database. Where a match occurs, the traveller is referred to an immigration officer.

The Memorandum of Understanding

5.7 The Information Technology (IT) Annex to the MOU sets out the governing principles for the parties to actively cooperate to:

> Improve and develop information technology systems, databases and equipment wherever possible, and
>
> Develop and implement appropriate Key Performance Indicators (KPIs) to ensure the operational effectiveness of Primary Immigration Clearance activity.

5.8 In terms of managing the stakeholder relationship, the most significant elements of the MOU are the management of system performance through reporting requirements and the communication provisions.

5.9 The MOU generally provides for the development of systems related reports 'to inform operational effectiveness of primary immigration clearance activity and system availability'. Thirteen individual reports are listed in the IT Annex to the MOU, 12 to be provided by Customs and one from DIBP at varying timeframes. The two agencies have been working together to develop the reports. As discussed in Chapter 4, DIBP advised that reporting requirements have not been finalised pending resolution of the reporting specifications (report definitions document) and the capacity of Customs to deliver the reports. At the time of writing this report, DIBP advised that discussions are still ongoing and 'all parties are committed to establishing regular and accurate reporting as outlined in the MOU'.

5.10 The lack of the systems related reports as required under the MOU means that the two agencies do not have access to information about operational effectiveness of primary immigration clearance activity and system availability.

Key performance indicators

5.11 The MOU and the IT Annex both require that key performance indicators (KPIs), as agreed between the parties, be developed. DIBP drafted KPIs but these have not yet been signed off by Customs.

5.12 DIBP has also developed detailed reporting criteria for each of the reports required under the MOU but these have also not been signed off by Customs. Given the slow progress of this aspect of CMAL's operations, the ANAO considers that close management oversight will be necessary to bring this activity to a successful conclusion.

Communication provisions

5.13 The MOU provides for communications between the agencies on a number of levels. At senior executive level, DIBP and Customs have established a Deputy Secretaries Steering Committee, which meets twice yearly to discuss matters relevant to border processing (for example, the development of key performance indicators) and other significant strategic initiatives, such as progress with the introduction of biometrics. This committee has met regularly, at approximately six monthly intervals, over the last two years, although CMAL specific matters are more likely to be discussed in the Passenger Business Systems Working Group (PBSWG).

5.14 The PBSWG includes representatives from both agencies. The group's monthly meetings cover operational issues relating to information technology. The ANAO's review of the minutes of the group's meetings indicate that the issues discussed included: the outages report prepared by DIBP for Customs; the report definitions document referred to in paragraph 5.9; the implications for Customs of the data refresh project (discussed at paragraph 5.23); systems maintenance issues which might impact on operations; and the ongoing role of the group.

5.15 Customs has advised that relationships between support officers in each agency have been strengthened through the activity required to support the recent data quality project, stating:

> Each agency has an improved understanding of how systems workload and performance impacts on both the efficiency and effectiveness of primary immigration clearance activities.

The Australian Security Intelligence Organisation

5.16 ASIO is a primary external stakeholder in CMAL, with an active interest in a large proportion of PAL records. The relationship between DIBP and ASIO is also underpinned by an MOU, which sets out the parameters of the relationship, reporting obligations and communication arrangements.

5.17 The ANAO was advised by both DIBP and ASIO that senior executives at both agencies meet at six monthly intervals to discuss broader border security strategies and high-level issues. At an operational level, the BOC and BOSS regularly communicate with their counterparts at ASIO to discuss operational issues. These arrangements were used effectively during a recent data quality project, with both agencies maintaining close contact at strategic and operational levels to identify and resolve any performance issues resulting from the project. The minutes of the DIBP/ASIO Deputy Secretaries' meetings confirm that both agencies consider their relationship to be highly effective.

The Department of Foreign Affairs and Trade

5.18 DFAT is both a contributor to, and user of, CMAL through:

- the inclusion of documents on the (DAL);
- the inclusion of alerts in relation to ARC 18, United Nations travel sanctions, principally as a result of United Nations Security Council travel bans or an Australian Government decision.

5.19 DFAT's interactions with CMAL are indirect; DFAT forwards details of proposals, passports and individuals for listing on CMAL to DIBP. In the case of passports, these listings are often provided via letter or fax and sometimes on behalf of foreign governments. DFAT will propose listings on PAL of individuals to whom public interest criteria may apply. Listings on DAL relate to lost, stolen or fraudulent travel documents as advised to DFAT by embassies, or documents held by people the subject of PAL alerts. Most DAL listings are prompted by DFAT.

5.20 DFAT's interest in individuals proposed for PAL alerts is usually because of their position or activities. The alerts relate to people wanted for war crimes, suspected of involvement in weapons of mass destruction, controversial visitors or UN sanctions, have been imposed against certain individuals. The ANAO's copy of the MAL database shows 6 807 alerts in ARC03 (war crimes), 2 860 alerts in ARC04 (controversial visitors and weapons of mass destruction) and 4 212 alerts in ARC18 (UN travel sanctions). The controversial visitors category generally comprises people about whom DFAT might want to be kept informed, but whose entry to Australia will not necessarily be denied.

5.21 DFAT does not have direct access to CMAL, but instead provides details to the relevant areas of DIBP, such as the controversial visitors unit. Liaison is primarily through quarterly meetings between DIBP and the sanctions and international crime area of DFAT, and ongoing contact in relation to data quality of proposed alerts. To date, the exchange of information between DIBP and DFAT has not been formalised in a written agreement. However, both agencies consider that the relationship is an effective one.

5.22 The decentralised nature of DFAT's operations is of concern to DIBP when dealing with CMAL referrals in relation to DFAT related ARCs. These referrals are either dealt with through the DIBP officer with responsibility for liaising with DFAT or by contacting DFAT directly. DIBP advised the ANAO that the decentralisation of DFAT operations is not always satisfactory from DIBP's perspective, as there is no single point of contact within DFAT for CMAL matters. It is anticipated that this issue will be resolved as part of formal agreement negotiations.

The Australian Federal Police

5.23 DIBP and the AFP have well established communications at the operational level and regular contact takes place between the AFP and the border security area. There are no regular meetings specific to CMAL.

5.24 The AFP provides supporting information to DIBP giving the reasons for foreign law enforcement inquiries. Such information may result in DIBP deciding to list on CMAL information about individuals who pose a border security risk as a result of criminal activity. Through its association with the international law enforcement community, the AFP facilitates DIBP's access to the Interpol database of wanted persons for the relevant details. Alerts for other law enforcement purposes are not entered into CMAL but are added to Custom's PACE system.

5.25 There are currently between almost 54 000 and 63 000 Interpol person alerts on CMAL. These equate to between just under 102 000 and

119 000 identities.[103] Interpol alerts raised for the first six months of 2013 are set out in Table 5.1.

Table 5.1: Interpol alerts raised between January–June 2013

Month	January	February	March	April	May	June
Interpol alerts	484	575	389	114	747	51

Source: DIBP monthly reports.

5.26 Interpol alerts are currently added to CMAL by BOC staff with the appropriate security clearance. Potential listings are evaluated by DIBP to determine whether the individuals are likely to present an immigration risk to Australia. If the individual is considered a risk, an alert under one of the ARCs related to criminal activity (05, 09 or 25) is raised. Should an Interpol notice be added to CMAL, the AFP is notified of any resulting matches.

Interpol requirements

5.27 The AFP requires DIBP to update CMAL alerts resulting from Interpol notices to reflect the most current information (and Interpol status) available. To this end, in 2011 DIBP reviewed CMAL's Interpol alerts against a list provided by Interpol and records were updated accordingly. An amended process has now been put in place whereby the AFP sends DIBP a daily summary of Interpol notices, containing all new, amended and cancelled notices processed the previous day for DIBP to update their records.

5.28 Interpol prescribes the circumstances under which national agencies can access and use data from the Interpol Information System.[104] New rules came into effect on 1 July 2013, and in relation to the review and retention of data, require:

- downloaded Interpol data to be updated at least once a week, including when such updating implies the deletion of data; and

[103] The figures are the result of two separate searches; a search of the PAL database for alerts with an 'Interpol alert' group code, which produces a figure of 54 000 records and a search of the narratives for the term 'Interpol', which produces a figure of 63 000 records.

[104] INTERPOL's Rules define 'download' as '… any operation involving the exportation of data from the INTERPOL Information System into another information system.'

- the downloaded data must be deleted when the purpose for which they were downloaded has been achieved and, at the very latest, when the period of six months has expired.

5.29 At present, DIBP does not have the procedures in place to comply with the weekly update requirement, and data is sometimes retained on the CMAL system after the Interpol alert is removed, principally for character determination purposes. The retention of such data conflicts with Interpol requirements. The AFP has advised the ANAO that an inaugural User Agreement, covering the Interpol rules, has been drafted by the AFP and is currently with DIBP for signature. DIBP has advised that the User Agreement will be considered in the light of the overarching strategic plan for CMAL.

5.30 DIBP has commenced an IT project to integrate DIBP and AFP systems to search across Interpol's databases via the AFP connection, which will allow Interpol notices to be searched directly for visa applicants and travellers.

5.31 DIBP has advised that there are signed Heads of Agreement in place with both both DFAT and the AFP, with Service Schedules which detail a range of specific procedures. The Service Schedule with DFAT relating to access to CMAL is under negotiation and will sit alongside Service Schedules governing DFAT access to other DIBP systems.

Conclusion

5.32 DIBP has developed close collaborative and effective working relationships with ASIO and Customs. The relationships are underpinned by MOUs, which provide an appropriate operating framework, both in terms of access to information and communication arrangements. DIBP and Customs have been slow to develop appropriate systems reporting arrangements as specified in the annex to the MOU but are currently working together to resolve this issue. ASIO and DIBP also have a close and effective working relationship that is underpinned by the MOU between the two agencies. Relationships with the AFP and DFAT are necessarily less extensive but still effective in terms of the operation of CMAL. Steps are also being taken to formalise these arrangements.

6. Managing Certain CMAL Alerts

This chapter examines DIBP's management of the listing of Australian citizens and children on CMAL.

Introduction

6.1 Under the *Migration Act 1958*, Australian citizens are generally free to travel from and return to Australia at will; DIBP has no authority to detain Australians at the border without their permission. A listing on CMAL can result in travellers being delayed at the Australian border, pending an identity check. A listing on DAL can mean they are prevented from travelling from departure ports worldwide. Consequently, listing of Australians on CMAL is a serious matter and requires sound administrative controls. Similarly, particular care should be taken in listing the identities of children, who generally have higher levels of dependency on other people and who may be listed for reasons of their family relationship alone.

6.2 The ANAO examined DIBP's management of the listing of these two groups on CMAL.

Listing of Australian citizens on CMAL

6.3 The 2008 audit found serious deficiencies in DIBP's procedures in relation to listing Australian citizens on MAL. In particular, its failure: to have a coherent policy on inclusion of Australians on MAL; to cull MAL records; and to allocate clear responsibility for the records. The 2008 audit made the following recommendation:

ANAO Report No.35 2008–09: Recommendation No. 2

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.

6.4 The department's policies for including Australians on MAL were described in the 2008 audit as being neither 'coherent nor complete'. Further, the department had not fully clarified its reasons for wanting Australians on MAL and had not identified the characteristics which would justify their inclusion.[105] In response to the 2008 audit, the department set out the policy for placing Australians on MAL in an internal minute in September 2009. The minute was comprehensive and clarified the:

- policy basis for listing Australians on PAL and documents belonging to Australians on DAL;
- current status of PAL and DAL records, including numbers of records and recent review activity;
- need to place Australians on PAL where documents have been lost in transit;
- need for an ongoing review strategy for Australians on CMAL; and
- matching of PAL records with the passport database and Integrated Client Services Environment (ICSE) to determine citizenship status.

6.5 More recently, DIBP advised in its submission to the ANAO, that its listing of Australians on CMAL is now tightly controlled by appropriate procedures that include the:

- policy parameters governing the listing of Australians in CMAL being clearly outlined in the CMAL PAM3;
- requirements for prior approval for the listing from a senior officer; and
- requirements for the narrative text of the listing to include information about the status of Australians and the need for their permission prior to detaining them at the border for anything other than an identity check.

6.6 DIBP allocated responsibility for managing the records of Australians on CMAL to the Intelligence and Analysis Section (IAS), the owner of ARC07 (serious criminal) alert records. The majority of Australian identities are allocated against this ARC. The IAS works with the Data Management and

[105] ANAO, Audit Report No. 35, 2008–09, op cit, p.88.

Reporting Team (DMRT) in the BOSS to regularly review records of Australians on CMAL.

6.7 DIBP undertook a comprehensive review of Australians on CMAL in mid-2008, during the conduct of the previous ANAO audit, and again in May 2009. The 2008 review enabled DIBP to significantly reduce its listings of Australians on CMAL and this reduction continued after the May 2009 review. In this latter review, DIBP matched the PAL records against the Australian Passport database and ICSE to determine citizenship status and found 1 436 records with Australian citizenship. By July 2009 MAL contained just over 200 unique Australian identities, down from over 500 in November 2007. As at 10 May 2013, there were 172 unique Australian identities listed on CMAL.

DIBP's current policies and procedures for listing Australians on CMAL

6.8 The policy guidance is set out in the CMAL PAM3 and provides that, generally, Australian identities can only be considered for listing on PAL if credible information exists to suggest that they intend to commit or to facilitate breaches of the *Migration Act 1958* or have already been convicted of doing so. For example, Australians are listed on PAL where they have:

- been involved in immigration fraud or malpractice; or
- been involved as a sponsor of an applicant under irregular circumstances.

6.9 Australian documents can be listed on DAL if there is a view or concern that a particular document may be used improperly because an Australian has:

- had credentials lost or stolen and it is strongly suspected that the identity may be misused for gaining access to Australia; or
- presented a badly damaged document which is to be impounded on arrival under the *Passport Act 2005*.

6.10 The CMAL PAM3 emphasises that it is not permissible to delay an Australian citizen who is listed on PAL at the Australian border without their permission, once their identity has been confirmed and a face to passport check has been completed. A listing on DAL, however, may prevent boarding of a flight or vessel elsewhere in the world.

Administrative controls

6.11 The individual ARC entries in the CMAL PAM3 identify whether Australians can or cannot be listed against the ARC, with the exception of national security alerts, where no guidance is provided. Australians can be listed against the following ARC categories:

- ARC07 (organised immigration malpractice); and
- ARC17 (lost or stolen travel document).

6.12 For Australians to be listed under ARC07, the proposer must obtain approval from the Director, IAS. Senior Executive level approval must be obtained for Australian documents to be listed on the DAL, given the serious nature of the consequences for the Australian traveller.

6.13 ANAO analysis of the copy of the CMAL database as at November 2012 showed that the database included:

- 253 Australian records, corresponding to 250 identities (and 182 unique individuals) listed on PAL (as at 18 July 2008, there were 772 records of Australian citizens on MAL);
- six Australian children are listed, including one listed against ARC08, which should only include non-Australian children;
- 368 travel documents related to Australians listed on DAL;
- Australian identities were also listed against ARCs 5, 6, 8 10, 12, 13 and 14;
- of the records listed on PAL, 235 are listed against ARC categories 01, 07 and 17. There are therefore 18 identities assigned to the incorrect ARC; and
- of the 182 unique individuals listed, the narratives for 141 of these individuals were missing the required permissions notation as required in the CMAL PAM3.

6.14 Recent advice from DIBP shows that, as at 10 May 2013, Australians were listed against the national security ARC and ARCs 07 and 17 only.

IAS procedures

6.15 The IAS, the ARC07 owner, has developed a standard operating procedure (SOP) governing the listing of Australian citizens and documents on

CMAL, including the reasons why an Australian identity or a travel document belonging to an Australian can be listed and the approval processes required.

6.16 The CMAL PAM3 and the SOPs in use by the IAS provide conflicting advice about the listing of Australians on the database. The SOP infers that proposers of PAL alerts should use either the ARC07 (organised immigration malpractice) or ARC13 (immigration malpractice) codes. The CMAL PAM3 instruction states that Australians are not to be listed against ARC13, although it does not give any policy explanation for this statement. DIBP was unable to provide advice to the ANAO as to why both the ARC07 and ARC13 categories existed, when they appeared to cover the same subject matter, and why Australians could be listed in one category and not the other.

6.17 In practice, Australians have been routinely listed against ARC13 and the twice yearly reports generated by the DMRT on Australians on CMAL for the IAS are generated against ARCs 07 and 13. Having been alerted to this deviation from the CMAL PAM3 instruction, DIBP reviewed the ARC13 entries and has either moved them to ARC07 or 'end dated' the entries so that they would be removed from the database at the next automatic expiry run. The ANAO has been informed that the procedures have been amended to reflect the CMAL PAM3 advice, to reduce the risk that Australians will be listed against an incorrect ARC category in future.

Narrative requirements for Australian listings

6.18 As previously noted, narrative requirements are important in the case of Australian identities on CMAL because they guide DIBP staff on the appropriate border procedures for Australians listed on CMAL. The CMAL PAM3 and the SOPs emphasise that DIBP officers have no authority to delay or question Australian citizens in immigration clearance without their consent and it is important that the narrative reflects this fact.

6.19 The IAS SOP is confusing because the suggested narrative is able to be 'amended as appropriate'. The proposer of the alert could misinterpret the narrative instruction and omit the permissions clause. Although the Australians on PAL checklist in the CMAL PAM3 requires the DIBP officer to include the additional narratives for Australians, the use of that checklist is not mandatory and the checklist is not required to be signed off by a more senior staff member or BOC officer.

6.20 The ANAO analysed the narratives in the listings of Australians on the ANAO's copy of the CMAL database. The ANAO found there were

397 narratives associated with identities that have Australian citizenship listed on CMAL[106], of which:

- 84 narratives contained the disclaimer information as required by the CMAL PAM3; and
- the remaining 313 narratives did not contain this disclaimer.

6.21 Of the 182 individuals with Australian citizenship on ANAO's copy of the CMAL database, only 41 (22 per cent) had a narrative for at least one of the identities associated with that person, containing the correct information.[107]

6.22 There are 564 DAL listings with a nationality of Australian, 368 of which are not associated with an identity record and are listed on DAL only. There are 396 narratives associated with the 368 records (each record can contain a number of narratives), of which 363 do not have the required information, that is only 33 (8.3 per cent) contain the suggested narrative.

6.23 Consequently, while there is explicit guidance in the CMAL PAM3 about the content of the narrative for Australian records in CMAL, the ANAO found that the proportion of non-compliant narratives in the PAL and the DAL for Australian citizens is high. This level of non-compliance is of concern, particularly as a listing on DAL can mean Australians are prevented from boarding at overseas ports. DIBP advises that the consequences of the omission from the narratives of the recommended text is mitigated by the fact that border staff are well versed in what is required of them when they are dealing with Australians at the border.

Review of Australians on CMAL

6.24 DIBP's policy is that all Australian identities listed on CMAL must be reviewed every 12 months to test whether the reasons for listing are still current and relevant. The IAS reviews the records listing against ARCs 07 and 13, while the BOC is responsible for reviewing all other Australian identity records in consultation with the ARC owner. BOC staff are required to check DFAT systems on a regular basis for Australian documents and remove them from CMAL if appropriate.

[106] Some identities have multiple narratives.

[107] The figures cited in this paragraph are derived from the copy of the CMAL database provided to the ANAO in November, 2012.

6.25 The DMRT develops the following reports to identify Australian citizens listed on CMAL:

- a twice yearly check to compare the Australian Passport database with the PAL database to identify PAL alerts potentially belonging to Australian citizens;
- a monthly report to identify likely errors emanating from alert records approved through the RIF;
- a twice yearly CMAL report (CMAL005 report) which provides details of Australian citizens on PAL (ARCs 07 and 13) to the IAS; and
- ad-hoc reports where a search within the narrative field for terms such as 'citizenship granted' and 'not relevant to citizenship' is undertaken.

6.26 The passport database check identifies those new citizens who have applied for a passport, but only those new citizens. There is no other formalised process by which the BOC is notified of persons attaining citizenship.

Conclusion

6.27 The 2008 audit recommendation has been largely implemented. DIBP has sought to address concerns about Australians on CMAL by clarifying the policy justification for listing Australians and including procedural advice in the CMAL PAM3 to make sure that Australian listings remain relevant and accurate. Reviews in 2008 and 2009 have reduced the number of Australians listed on CMAL from 500 in November 2007 to 172 in May 2013. DIBP undertakes regular reviews of Australians on CMAL to ensure listings are relevant and current.

6.28 However, a residual concern is the high proportion of the narratives in the alerts which are not compliant with the CMAL PAM3 requirement for the permission warnings and the inability of DIBP staff to detain or delay Australians at the border without permission, once identity is established.

Listing of children on CMAL

6.29 DIBP has no policies to guide staff about the listing of children on CMAL. All ARC categories contain a business rule of 'no minimum age' for an alert to be raised, which means that anyone under the age of 18, legally a child, can be listed against any ARC. CMAL contains a large number of alerts for children, throughout the PAL database, as identified in Table 6.1.

Table 6.1: Children on PAL (Under 18)

ARC		Number of records	Number of identities
03	War crimes/human rights abuses	2	2
04	Controversial visitors/weapons of mass destruction	18	15
05	Serious or high profile crime	49	35
06	Health concerns	2 576	2 351
07	Organised immigration malpractice	306	169
08	Child custody concerns	2 896	1 919
09	Other criminal	92	75
10	Overstayers	1 280	906
11	Breach of visa conditions	96	71
12	Debt to the Commonwealth	1 315	748
13	Immigration malpractice	303	229
14	Refusal/bypass immigration clearance	792	316
16	Suspect genuineness	375	316
17	Surrender Australian travel document	0	0
18	Travel sanctions	63	56
19	Illegal fishers	18	12
20	False or misleading immigration/skilled migration fraud	168	125
25	Serious criminal – poor biodata	3	3
Total		**10 532**	**7 524**[108]

Source: ANAO analysis of copy of CMAL database.

6.30 The ANAO's analysis of the copy of the CMAL database found that there are approximately 10 500 alerts for children listed on PAL, corresponding to 7 250 unique individuals. Children are listed against all ARC categories, except for ARC17, surrender Australian travel document. Some 2 500 children are listed under health concerns and almost 3 000 children are listed under child custody concerns. In addition, 1 315 children are listed on CMAL for debts to the Commonwealth (ARC12).

[108] The total number shown here will not match the number of unique children on CMAL as some children are listed for multiple ARCs.

6.31 The ANAO notes that these listings are often required by the terms of certain treaties or United Nations requirements. For example, United Nations travel sanctions will apply to the whole family. DIBP also lists children where there is a debt to the Commonwealth but that debt may have been incurred by a parent.

6.32 The following case study illustrates how, for one of the groupings, listing of children may pose a risk.

Case study: ARC12 Debts to the Commonwealth

ARC12 lists individuals who have a debt to the Commonwealth, which includes costs incurred for immigration detention or removal from Australia, litigation costs, and social security debts. The ANAO's copy of CMAL contains a total of 61 457 alerts in ARC12, including 1 315 alerts for children, corresponding to 748 persons. While a child cannot incur a debt to the Commonwealth for deportation and removal costs[109], a child who has costs awarded against him or her in the Refugee Review Tribunal can incur debts and, as a result, can be listed in CMAL under ARC12. The ANAO was able to identify numerous instances of minors as young as three listed on CMAL with debts to the Commonwealth for legal costs.

DIBP has advised that a child might also be listed if the parents had incurred a debt, even though the debt did not attach to the child. The ANAO notes that in these circumstances the debt properly attaches to the parent and not the child and it is the parent who should be the subject of an alert on CMAL and not the child.

An additional concern relates to the length of time alerts remain on the MAL database. Because the default review and expiry rules for ARC12 alerts may be for prolonged periods, it is possible that children's records are retained in the database for decades. For example, the default expiry period for a debt greater than $1 000 is 100 years of age. It is conceivable that the child, who may be unaware of any debt problems, at a later date could seek to return to Australia before the expiration of the alert. A visa application in these circumstances will prompt a CMAL status of amber or red and potentially disrupt the application process.

In the period 2011 to June 2013, ARC12 alerts resulted in 28 741 overrides (that is, visa applications proceeded for further consideration). This figure amounted to 25.19 per cent of total overrides during the period. The only ARC category higher was ARC06, health concerns.

[109] *Migration Act 1958* (Cth), s 212 (2) and (3).

Conclusion

6.33 While there is a large number of children listed on the PAL database across a range of ARCs, many of these listings are requirements of international agreements or legislation. Given that children listed on CMAL will remain on the system for extensive time periods, with only child custody records expiring at the age of 18 years, particular care should be taken to make sure that such entries are appropriate. There would be merit in DIBP clarifying the circumstances where it is appropriate to list children on CMAL and developing rules to guide DIBP staff when listing children.

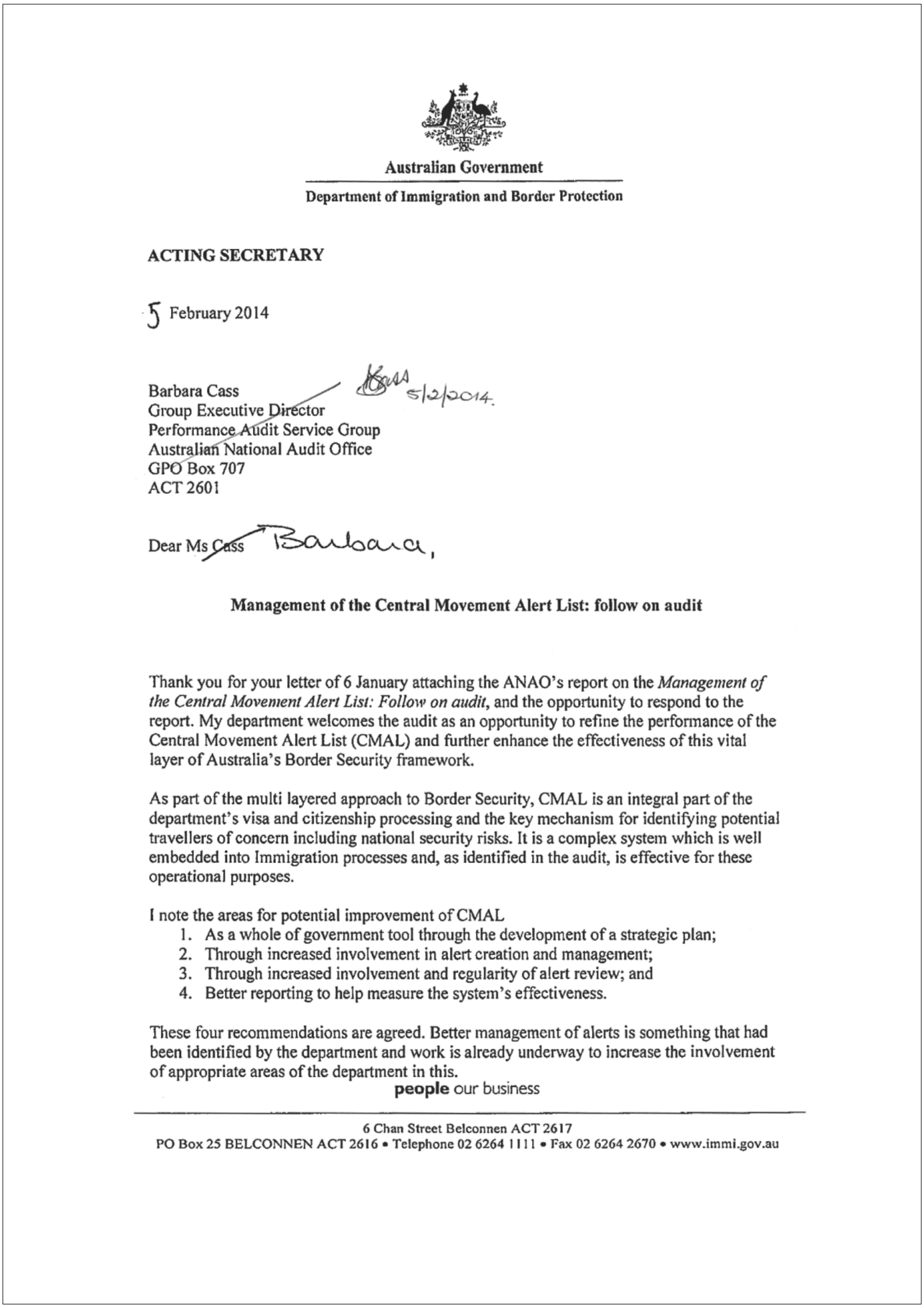
6.34 There is also a small number of Australian children listed on the PAL database. Policies applying generally to the listing of Australians should be applied to these records and, where the children themselves do not fit the criteria, the records removed.

Ian McPhee
Auditor-General

Canberra ACT
20 February 2014

Appendices

Appendix 1: Agency response to proposed report



Australian Government

Department of Immigration and Border Protection

ACTING SECRETARY

5 February 2014

Barbara Cass
Group Executive Director
Performance Audit Service Group
Australian National Audit Office
GPO Box 707
ACT 2601

5/2/2014.

Dear Ms ~~Cass~~ Barbara,

Management of the Central Movement Alert List: follow on audit

Thank you for your letter of 6 January attaching the ANAO's report on the *Management of the Central Movement Alert List: Follow on audit*, and the opportunity to respond to the report. My department welcomes the audit as an opportunity to refine the performance of the Central Movement Alert List (CMAL) and further enhance the effectiveness of this vital layer of Australia's Border Security framework.

As part of the multi layered approach to Border Security, CMAL is an integral part of the department's visa and citizenship processing and the key mechanism for identifying potential travellers of concern including national security risks. It is a complex system which is well embedded into Immigration processes and, as identified in the audit, is effective for these operational purposes.

I note the areas for potential improvement of CMAL

1. As a whole of government tool through the development of a strategic plan;
2. Through increased involvement in alert creation and management;
3. Through increased involvement and regularity of alert review; and
4. Better reporting to help measure the system's effectiveness.

These four recommendations are agreed. Better management of alerts is something that had been identified by the department and work is already underway to increase the involvement of appropriate areas of the department in this.

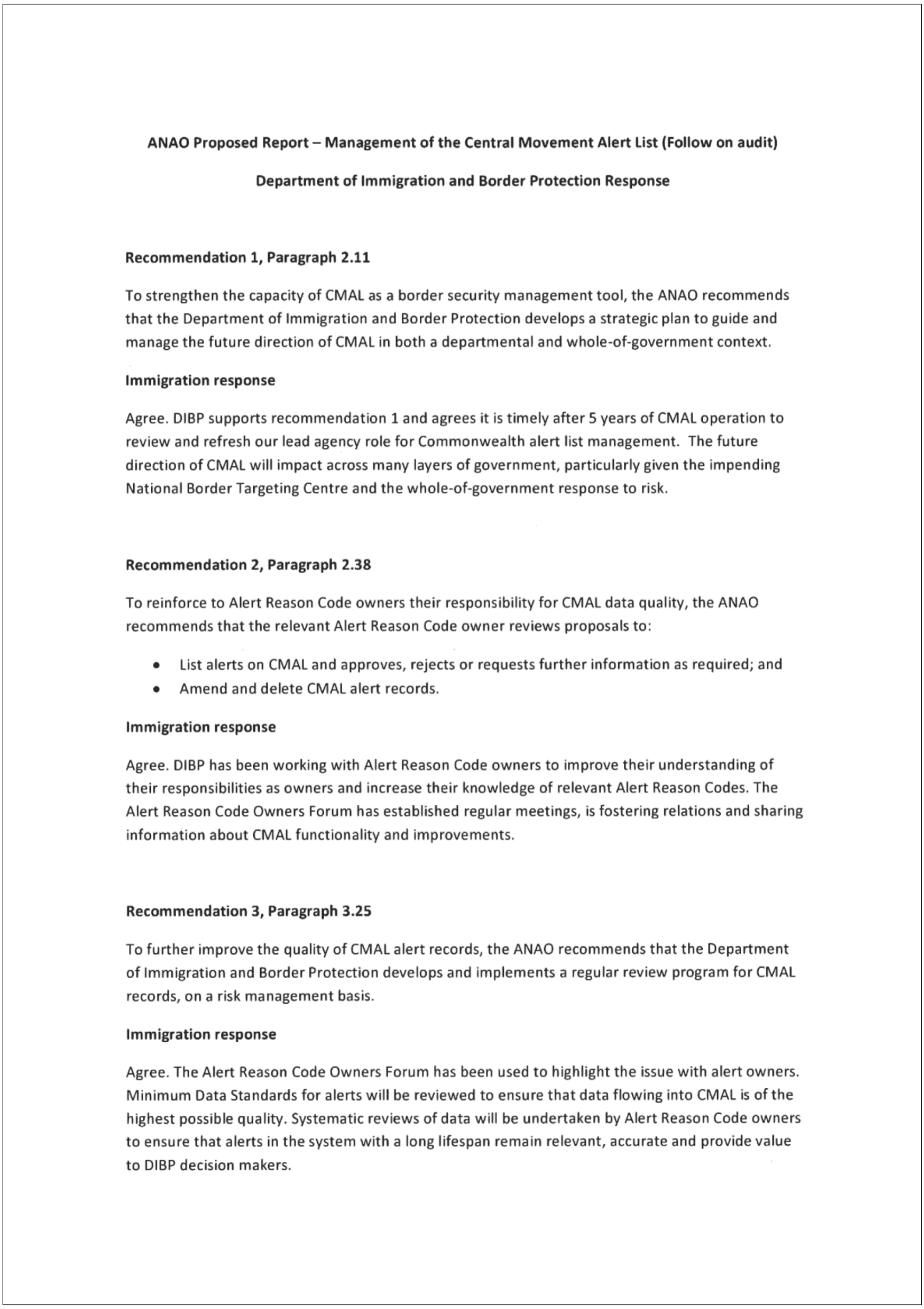
people our business

6 Chan Street Belconnen ACT 2617
PO Box 25 BELCONNEN ACT 2616 • Telephone 02 6264 1111 • Fax 02 6264 2670 • www.immi.gov.au

Attached to this letter is a more detailed response to each of the recommendations and the overall report.

Yours sincerely

Liz Cosson AM CSC



ANAO Proposed Report – Management of the Central Movement Alert List (Follow on audit)

Department of Immigration and Border Protection Response

Recommendation 1, Paragraph 2.11

To strengthen the capacity of CMAL as a border security management tool, the ANAO recommends that the Department of Immigration and Border Protection develops a strategic plan to guide and manage the future direction of CMAL in both a departmental and whole-of-government context.

Immigration response

Agree. DIBP supports recommendation 1 and agrees it is timely after 5 years of CMAL operation to review and refresh our lead agency role for Commonwealth alert list management. The future direction of CMAL will impact across many layers of government, particularly given the impending National Border Targeting Centre and the whole-of-government response to risk.

Recommendation 2, Paragraph 2.38

To reinforce to Alert Reason Code owners their responsibility for CMAL data quality, the ANAO recommends that the relevant Alert Reason Code owner reviews proposals to:

- List alerts on CMAL and approves, rejects or requests further information as required; and
- Amend and delete CMAL alert records.

Immigration response

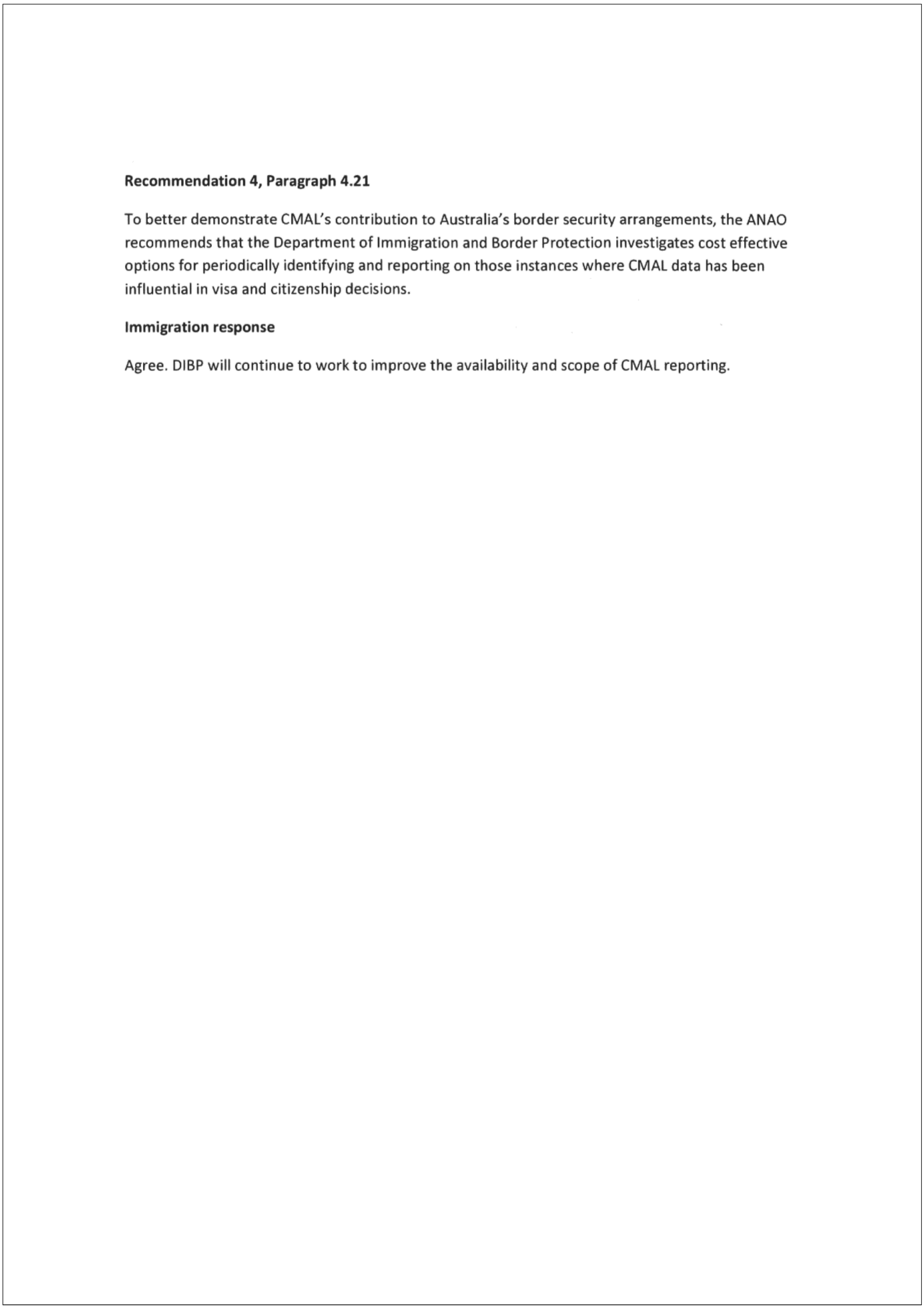
Agree. DIBP has been working with Alert Reason Code owners to improve their understanding of their responsibilities as owners and increase their knowledge of relevant Alert Reason Codes. The Alert Reason Code Owners Forum has established regular meetings, is fostering relations and sharing information about CMAL functionality and improvements.

Recommendation 3, Paragraph 3.25

To further improve the quality of CMAL alert records, the ANAO recommends that the Department of Immigration and Border Protection develops and implements a regular review program for CMAL records, on a risk management basis.

Immigration response

Agree. The Alert Reason Code Owners Forum has been used to highlight the issue with alert owners. Minimum Data Standards for alerts will be reviewed to ensure that data flowing into CMAL is of the highest possible quality. Systematic reviews of data will be undertaken by Alert Reason Code owners to ensure that alerts in the system with a long lifespan remain relevant, accurate and provide value to DIBP decision makers.



Recommendation 4, Paragraph 4.21

To better demonstrate CMAL's contribution to Australia's border security arrangements, the ANAO recommends that the Department of Immigration and Border Protection investigates cost effective options for periodically identifying and reporting on those instances where CMAL data has been influential in visa and citizenship decisions.

Immigration response

Agree. DIBP will continue to work to improve the availability and scope of CMAL reporting.

Appendix 2: Table of ANAO Report No 35, 2008–09 recommendations and DIBP progress in addressing these recommendations

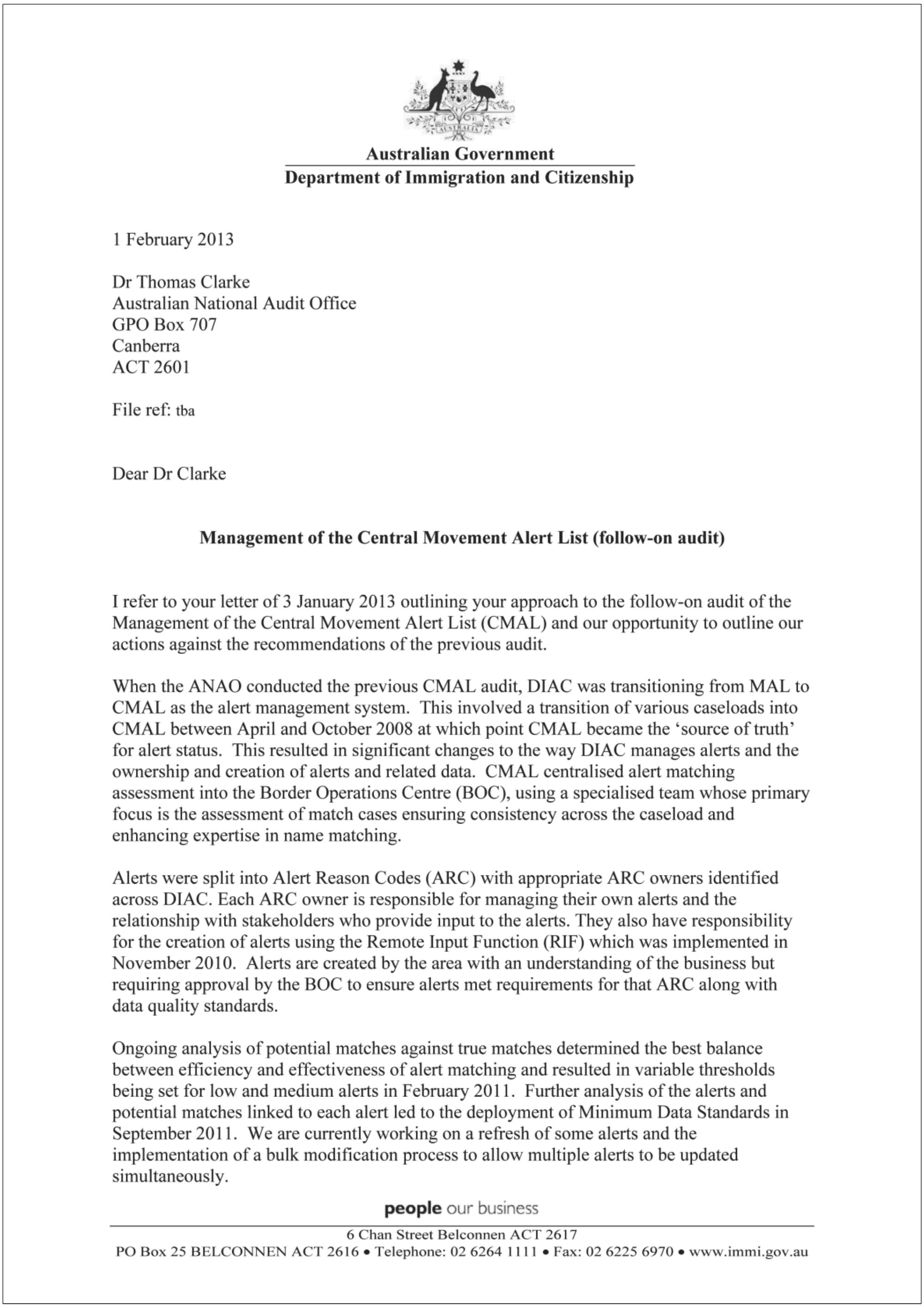
Recommendation	Action taken by DIBP	ANAO comment on DIBP actions
Recommendation 1		**Partially implemented**.
The ANAO recommends that DIAC develop a plan for the population, maintenance and review of the MAL database.	No action by DIBP.	There is no CMAL data management plan.
[The plan] should include, 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	ARC ownership responsibilities have been defined and set out in CMAL PAM3. Minimum data standards have been amended and set out in CMAL PAM3. Business rules have been established.	This part of the recommendation has been addressed. However, while the ARC ownership rules have been clearly defined, operational procedures developed within the Borders Operations Branch have not been inclusive of involving ARC owners in activities which promote responsibility for CMAL data.
• 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.	The Remote Input Function (RIF) requires that all proposed alerts are reviewed for compliance with the CMAL PAM3 by the BOC. Review and expiry periods for alert records have been determined and set out in CMAL PAM3.	Review of RIF inputs by the BOC is not quality tested. ARC owners have little practical responsibility for oversighting data quality. There is no program with target dates for data cleansing of CMAL records and no mechanism for reviewing and reporting progress with this work.

Recommendation	Action taken by DIBP	ANAO comment on DIBP actions
Recommendation 2		**Implemented**
The ANAO recommends that DIAC: - clarifies the circumstances in which it can properly record Australian citizens on MAL, consulting with other agencies with an interest in MAL as appropriate;	Policy outlined in CMAL PAM3. Permissible ARC categories set out in the CMAL PAM3.	The policy guidelines set out in the CMAL PAM3 have been rationalised. For example each ARC is explicit about whether Australians can be included and the manual sets out the requirements for the narratives when listing Australian identities.
- in this light, revises it policy and procedural guidelines for recording Australian citizens on MAL; and	CMAL PAM3 contains policy and operational guidance on listing Australians on the database.	
- completes its review of records of Australians on MAL, and deletes records of Australians where they are inappropriately recorded.	Records reviewed twice yearly for ARCs 07 and 13. Passport database interrogated twice yearly for Australian citizens.	
Recommendation 3		**Not implemented**
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.	No reporting of this kind is regularly undertaken by DIBP. DIBP pursued a project in 2010 to analyse the extent to which CMAL contributed to visa and citizenship decisions. This analysis has not been ongoing.	As discussed in Chapter 4, DIBP could undertake additional performance reporting measures, such as analysis of the narratives and override data, within current CMAL capabilities.

Recommendation	Action taken by DIBP	ANAO comment on DIBP actions
Recommendation 4		**Implemented**
To enable DIAC to manage MAL effectively, the ANAO recommends that DIBP seek to measure and report internally on: • data quality;	Data quality measurement and reporting is undertaken through the monthly RIF error report and the monthly report to ASIO on the most problematic national security alerts. All other alerts are not routinely reviewed.	
• MAL's reliability; and	DIBP has internal and external measures for CMAL's reliability. Internal measures primarily consist of systems performance reporting. The major external measure is the reporting arrangement set out in the Customs MOU IT Annex and reporting to ASIO	
• Client service, measured by the service level agreements agreed internally with CMAL client areas of the department.	DIBP has developed a service level agreement for the management of the queues internally within the department.	

Recommendation	Action taken by DIBP	ANAO comment on DIBP actions
Recommendation 5		**Partially implemented [pending finalisation of reporting under the Customs IT Annex.]**
DIBP implement a mechanism for providing regular assurance that all key parts of the MAL system are operating satisfactorily	Reporting mechanisms have been developed. Regular face to face meetings have been implemented with major stakeholders for the identification and consideration of CMAL systems issues.	Taken together, the reporting mechanisms for systems performance and arrangements between agencies to provide assurance that CMAL is working as it should are appropriate. When problems arise, timeframes, responsibility and communications are identified. Reporting arrangements under the DIBP-Customs MOU are being finalised.

Appendix 3: DIBP submission, 1 February 2013



Australian Government
Department of Immigration and Citizenship

1 February 2013

Dr Thomas Clarke
Australian National Audit Office
GPO Box 707
Canberra
ACT 2601

File ref: tba

Dear Dr Clarke

Management of the Central Movement Alert List (follow-on audit)

I refer to your letter of 3 January 2013 outlining your approach to the follow-on audit of the Management of the Central Movement Alert List (CMAL) and our opportunity to outline our actions against the recommendations of the previous audit.

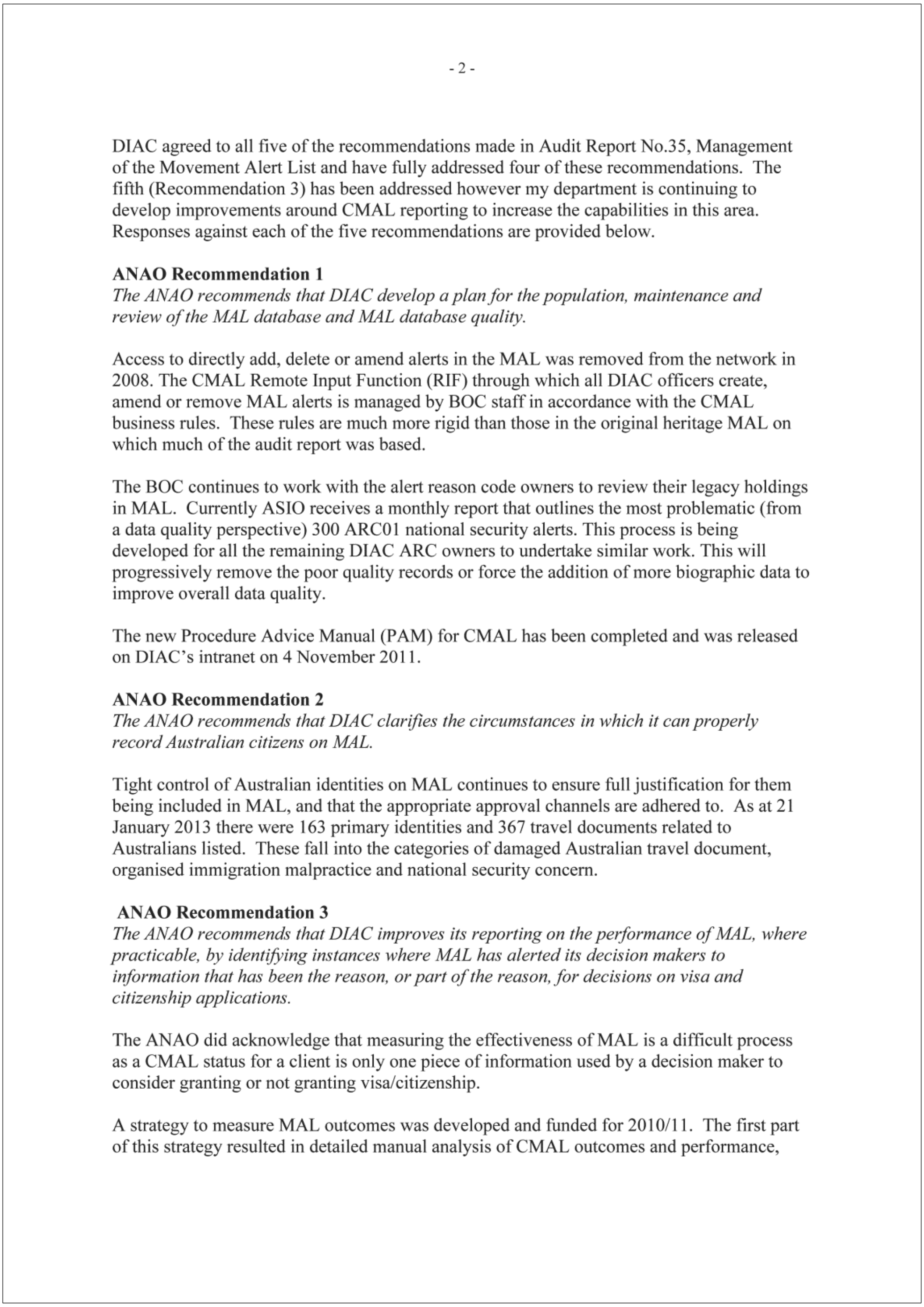
When the ANAO conducted the previous CMAL audit, DIAC was transitioning from MAL to CMAL as the alert management system. This involved a transition of various caseloads into CMAL between April and October 2008 at which point CMAL became the 'source of truth' for alert status. This resulted in significant changes to the way DIAC manages alerts and the ownership and creation of alerts and related data. CMAL centralised alert matching assessment into the Border Operations Centre (BOC), using a specialised team whose primary focus is the assessment of match cases ensuring consistency across the caseload and enhancing expertise in name matching.

Alerts were split into Alert Reason Codes (ARC) with appropriate ARC owners identified across DIAC. Each ARC owner is responsible for managing their own alerts and the relationship with stakeholders who provide input to the alerts. They also have responsibility for the creation of alerts using the Remote Input Function (RIF) which was implemented in November 2010. Alerts are created by the area with an understanding of the business but requiring approval by the BOC to ensure alerts met requirements for that ARC along with data quality standards.

Ongoing analysis of potential matches against true matches determined the best balance between efficiency and effectiveness of alert matching and resulted in variable thresholds being set for low and medium alerts in February 2011. Further analysis of the alerts and potential matches linked to each alert led to the deployment of Minimum Data Standards in September 2011. We are currently working on a refresh of some alerts and the implementation of a bulk modification process to allow multiple alerts to be updated simultaneously.

people our business

6 Chan Street Belconnen ACT 2617
PO Box 25 BELCONNEN ACT 2616 • Telephone: 02 6264 1111 • Fax: 02 6225 6970 • www.immi.gov.au



DIAC agreed to all five of the recommendations made in Audit Report No.35, Management of the Movement Alert List and have fully addressed four of these recommendations. The fifth (Recommendation 3) has been addressed however my department is continuing to develop improvements around CMAL reporting to increase the capabilities in this area. Responses against each of the five recommendations are provided below.

ANAO Recommendation 1
The ANAO recommends that DIAC develop a plan for the population, maintenance and review of the MAL database and MAL database quality.

Access to directly add, delete or amend alerts in the MAL was removed from the network in 2008. The CMAL Remote Input Function (RIF) through which all DIAC officers create, amend or remove MAL alerts is managed by BOC staff in accordance with the CMAL business rules. These rules are much more rigid than those in the original heritage MAL on which much of the audit report was based.

The BOC continues to work with the alert reason code owners to review their legacy holdings in MAL. Currently ASIO receives a monthly report that outlines the most problematic (from a data quality perspective) 300 ARC01 national security alerts. This process is being developed for all the remaining DIAC ARC owners to undertake similar work. This will progressively remove the poor quality records or force the addition of more biographic data to improve overall data quality.

The new Procedure Advice Manual (PAM) for CMAL has been completed and was released on DIAC's intranet on 4 November 2011.

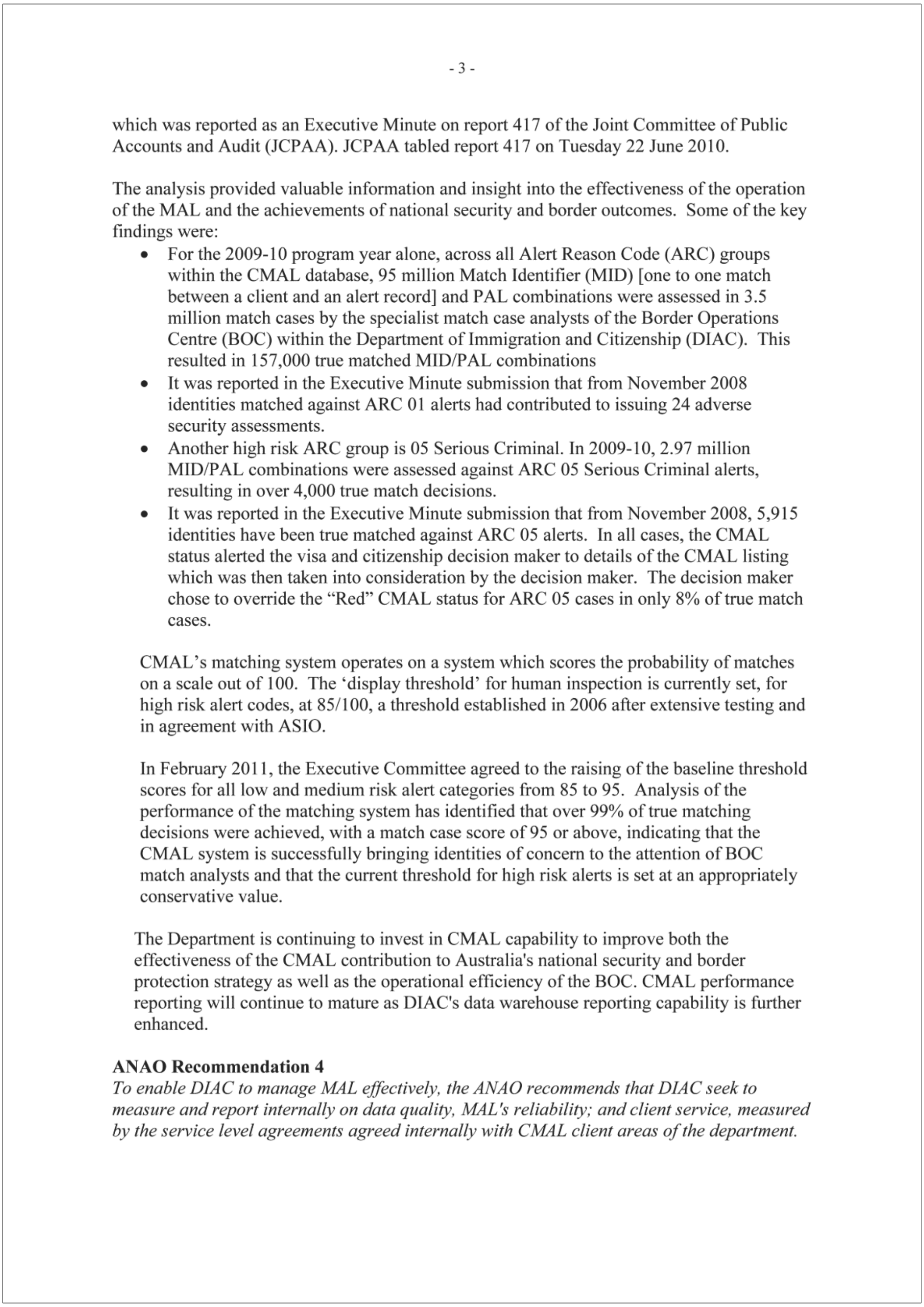
ANAO Recommendation 2
The ANAO recommends that DIAC clarifies the circumstances in which it can properly record Australian citizens on MAL.

Tight control of Australian identities on MAL continues to ensure full justification for them being included in MAL, and that the appropriate approval channels are adhered to. As at 21 January 2013 there were 163 primary identities and 367 travel documents related to Australians listed. These fall into the categories of damaged Australian travel document, organised immigration malpractice and national security concern.

ANAO Recommendation 3
The ANAO recommends that DIAC improves its reporting on the performance of MAL, where practicable, by 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.

The ANAO did acknowledge that measuring the effectiveness of MAL is a difficult process as a CMAL status for a client is only one piece of information used by a decision maker to consider granting or not granting visa/citizenship.

A strategy to measure MAL outcomes was developed and funded for 2010/11. The first part of this strategy resulted in detailed manual analysis of CMAL outcomes and performance,



which was reported as an Executive Minute on report 417 of the Joint Committee of Public Accounts and Audit (JCPAA). JCPAA tabled report 417 on Tuesday 22 June 2010.

The analysis provided valuable information and insight into the effectiveness of the operation of the MAL and the achievements of national security and border outcomes. Some of the key findings were:

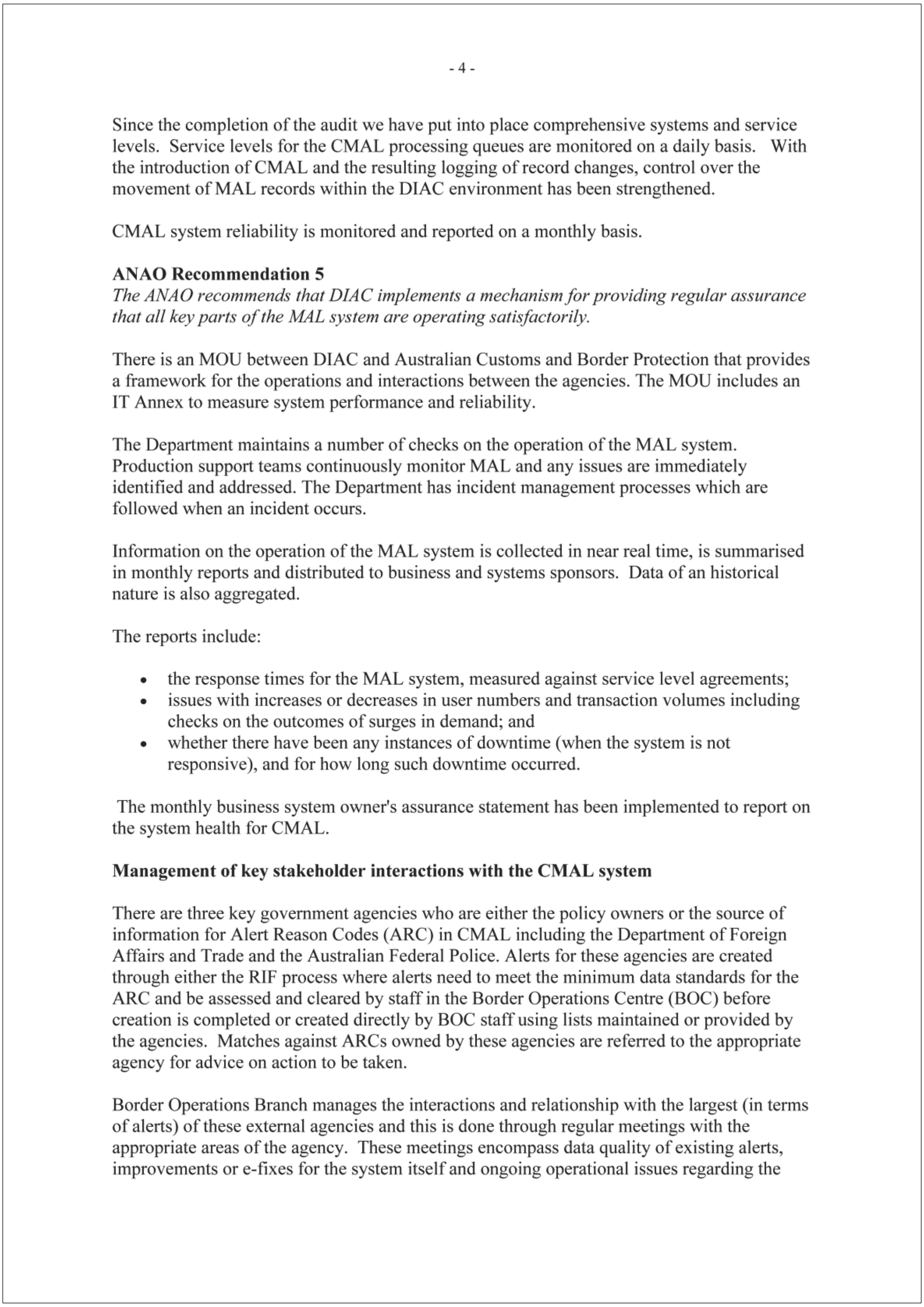
- For the 2009-10 program year alone, across all Alert Reason Code (ARC) groups within the CMAL database, 95 million Match Identifier (MID) [one to one match between a client and an alert record] and PAL combinations were assessed in 3.5 million match cases by the specialist match case analysts of the Border Operations Centre (BOC) within the Department of Immigration and Citizenship (DIAC). This resulted in 157,000 true matched MID/PAL combinations
- It was reported in the Executive Minute submission that from November 2008 identities matched against ARC 01 alerts had contributed to issuing 24 adverse security assessments.
- Another high risk ARC group is 05 Serious Criminal. In 2009-10, 2.97 million MID/PAL combinations were assessed against ARC 05 Serious Criminal alerts, resulting in over 4,000 true match decisions.
- It was reported in the Executive Minute submission that from November 2008, 5,915 identities have been true matched against ARC 05 alerts. In all cases, the CMAL status alerted the visa and citizenship decision maker to details of the CMAL listing which was then taken into consideration by the decision maker. The decision maker chose to override the “Red” CMAL status for ARC 05 cases in only 8% of true match cases.

CMAL’s matching system operates on a system which scores the probability of matches on a scale out of 100. The ‘display threshold’ for human inspection is currently set, for high risk alert codes, at 85/100, a threshold established in 2006 after extensive testing and in agreement with ASIO.

In February 2011, the Executive Committee agreed to the raising of the baseline threshold scores for all low and medium risk alert categories from 85 to 95. Analysis of the performance of the matching system has identified that over 99% of true matching decisions were achieved, with a match case score of 95 or above, indicating that the CMAL system is successfully bringing identities of concern to the attention of BOC match analysts and that the current threshold for high risk alerts is set at an appropriately conservative value.

The Department is continuing to invest in CMAL capability to improve both the effectiveness of the CMAL contribution to Australia's national security and border protection strategy as well as the operational efficiency of the BOC. CMAL performance reporting will continue to mature as DIAC's data warehouse reporting capability is further enhanced.

ANAO Recommendation 4
To enable DIAC to manage MAL effectively, the ANAO recommends that DIAC seek to measure and report internally on data quality, MAL's reliability; and client service, measured by the service level agreements agreed internally with CMAL client areas of the department.



Since the completion of the audit we have put into place comprehensive systems and service levels. Service levels for the CMAL processing queues are monitored on a daily basis. With the introduction of CMAL and the resulting logging of record changes, control over the movement of MAL records within the DIAC environment has been strengthened.

CMAL system reliability is monitored and reported on a monthly basis.

ANAO Recommendation 5
The ANAO recommends that DIAC implements a mechanism for providing regular assurance that all key parts of the MAL system are operating satisfactorily.

There is an MOU between DIAC and Australian Customs and Border Protection that provides a framework for the operations and interactions between the agencies. The MOU includes an IT Annex to measure system performance and reliability.

The Department maintains a number of checks on the operation of the MAL system. Production support teams continuously monitor MAL and any issues are immediately identified and addressed. The Department has incident management processes which are followed when an incident occurs.

Information on the operation of the MAL system is collected in near real time, is summarised in monthly reports and distributed to business and systems sponsors. Data of an historical nature is also aggregated.

The reports include:

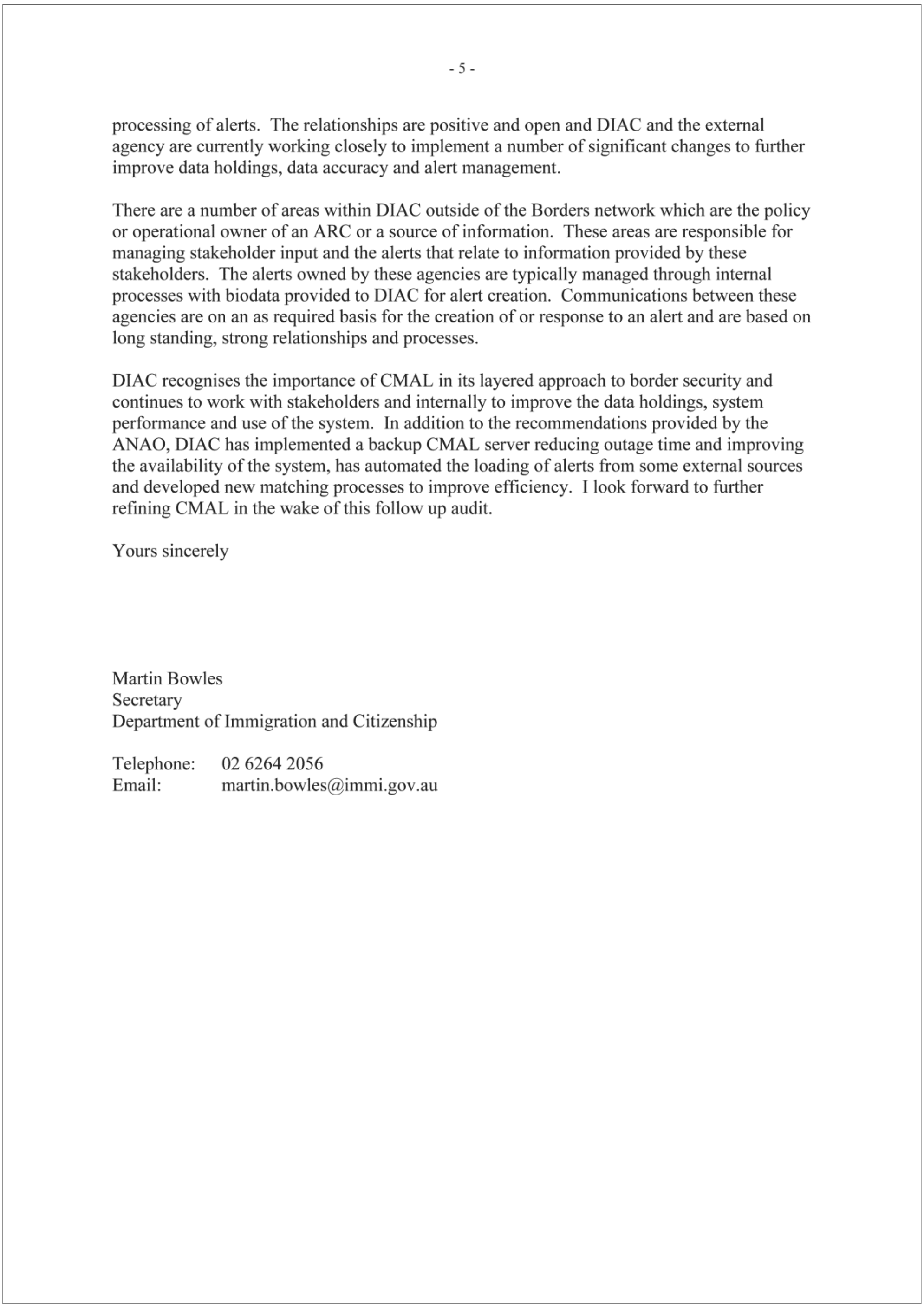
- the response times for the MAL system, measured against service level agreements;
- issues with increases or decreases in user numbers and transaction volumes including checks on the outcomes of surges in demand; and
- whether there have been any instances of downtime (when the system is not responsive), and for how long such downtime occurred.

The monthly business system owner's assurance statement has been implemented to report on the system health for CMAL.

Management of key stakeholder interactions with the CMAL system

There are three key government agencies who are either the policy owners or the source of information for Alert Reason Codes (ARC) in CMAL including the Department of Foreign Affairs and Trade and the Australian Federal Police. Alerts for these agencies are created through either the RIF process where alerts need to meet the minimum data standards for the ARC and be assessed and cleared by staff in the Border Operations Centre (BOC) before creation is completed or created directly by BOC staff using lists maintained or provided by the agencies. Matches against ARCs owned by these agencies are referred to the appropriate agency for advice on action to be taken.

Border Operations Branch manages the interactions and relationship with the largest (in terms of alerts) of these external agencies and this is done through regular meetings with the appropriate areas of the agency. These meetings encompass data quality of existing alerts, improvements or e-fixes for the system itself and ongoing operational issues regarding the



- 5 -

processing of alerts. The relationships are positive and open and DIAC and the external agency are currently working closely to implement a number of significant changes to further improve data holdings, data accuracy and alert management.

There are a number of areas within DIAC outside of the Borders network which are the policy or operational owner of an ARC or a source of information. These areas are responsible for managing stakeholder input and the alerts that relate to information provided by these stakeholders. The alerts owned by these agencies are typically managed through internal processes with biodata provided to DIAC for alert creation. Communications between these agencies are on an as required basis for the creation of or response to an alert and are based on long standing, strong relationships and processes.

DIAC recognises the importance of CMAL in its layered approach to border security and continues to work with stakeholders and internally to improve the data holdings, system performance and use of the system. In addition to the recommendations provided by the ANAO, DIAC has implemented a backup CMAL server reducing outage time and improving the availability of the system, has automated the loading of alerts from some external sources and developed new matching processes to improve efficiency. I look forward to further refining CMAL in the wake of this follow up audit.

Yours sincerely

Martin Bowles
Secretary
Department of Immigration and Citizenship

Telephone: 02 6264 2056
Email: martin.bowles@immi.gov.au

Index

Series Titles

ANAO Audit Report No.1 2013–14
Design and Implementation of the Liveable Cities Program
Department of Infrastructure and Transport

ANAO Audit Report No.2 2013–14
Administration of the Agreements for the Management, Operation and Funding of the Mersey Community Hospital
Department of Health and Ageing
Department of Health and Human Services, Tasmania
Tasmanian Health Organisation – North West

ANAO Audit Report No.3 2013–14
AIR 8000 Phase 2 – C-27J Spartan Battlefield Airlift Aircraft
Department of Defence

ANAO Audit Report No.4 2013–14
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2012 Compliance)
Across Agencies

ANAO Audit Report No.5 2013–14
Administration of the Taxation of Personal Services Income
Australian Taxation Office

ANAO Audit Report No.6 2013–14
Capability Development Reform
Department of Defence

ANAO Audit Report No.7 2013–14
Agency Management of Arrangements to Meet Australia's International Obligations
Across Agencies

ANAO Audit Report No.8 2013–14
The Australian Government Reconstruction Inspectorate's Conduct of Value for Money Reviews of Flood Reconstruction Projects in Queensland
Department of Infrastructure and Regional Development

ANAO Audit Report No.9 2013–14
Determination and Collection of Financial Industry Levies
Australian Prudential Regulation Authority
Department of the Treasury

ANAO Audit Report No.10 2013–14
Torres Strait Regional Authority – Service Delivery
Torres Strait Regional Authority

ANAO Audit Report No.11 2013–14
Delivery of the Filling the Research Gap under the Carbon Farming Futures Program
Department of Agriculture

ANAO Report No.12 2013–14
2012–13 Major Projects Report
Defence Materiel Organisation

ANAO Audit Report No.13 2013–14
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2013
Across Agencies

ANAO Audit Report No.14 2013-14

Explosive Ordnance and Weapons Security Incident Reporting
Department of Defence

ANAO Audit Report No.15 2013–14
The Indigenous Land Corporation's Administration of the Land Acquisition
Program Indigenous Land Corporation

ANAO Audit Report No.16 2013–14

Administration of the Smart Grid, Smart City Program
Department of the Environment
Department of Industry

ANAO Audit Report No.17 2013–14
Administration of the Strengthening Basin Communities Program
Department of the Environment

ANAO Audit Report No.18 2013–14
Administration of the Improving Water Information Program
Bureau of Meteorology

ANAO Audit Report No.19 2013–14
Management of Complaints and Other Feedback
Australian Taxation Office

ANAO Audit Report No.20 2013–14
Management of the Central Movement Alert List: Follow-on Audit
Department of Immigration and Border Protection

Current Better Practice Guides

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

Implementing Better Practice Grants Administration	Dec. 2013
Preparation of Financial Statements by Public Sector Entities	June 2013
Human Resource Management Information Systems – Risks and Controls	June 2013
Public Sector Internal Audit	Sept. 2012
Public Sector Environmental Management	Apr. 2012
Developing and Managing Contracts – Getting the right outcome, achieving value for money	Feb. 2012
Public Sector Audit Committees	Aug. 2011
Fraud Control in Australian Government Entities	Mar. 2011
Strategic and Operational Management of Assets by Public Sector Entities – Delivering agreed outcomes through an efficient and optimal asset base	Sept. 2010
Planning and Approving Projects – an Executive Perspective	June 2010
Innovation in the Public Sector – Enabling Better Performance, Driving New Directions	Dec. 2009
SAP ECC 6.0 – Security and Control	June 2009
Business Continuity Management – Building resilience in public sector entities	June 2009
Developing and Managing Internal Budgets	June 2008
Agency Management of Parliamentary Workflow	May 2008
Fairness and Transparency in Purchasing Decisions – Probity in Australian Government Procurement	Aug. 2007
Administering Regulation	Mar. 2007
Implementation of Program and Policy Initiatives – Making implementation matter	Oct. 2006