Canberra  ACT
17 June 2004

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in CrimTrac in accordance with the authority contained in the Auditor-General Act 1997. I present the report of this audit and the accompanying brochure to the Parliament. The report is titled The Implementation of CrimTrac.

Following its tabling in Parliament, the report will be placed on the Australian National Audit Office’s Homepage—http://www.anao.gov.au.

Yours sincerely

P. J. Barrett
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra  ACT
AUDITING FOR AUSTRALIA

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

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

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

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

http://www.anao.gov.au

Audit Team
Karen Sutcliffe
Kraig Lowes
David Crossley
Contents

Abbreviations/Glossary .................................................................................................................. 7

Summary and Recommendations .................................................................................................. 9

Executive Summary ...................................................................................................................... 11
  Background .......................................................................................................................... 11
  Key findings .......................................................................................................................... 11
  Overall audit conclusion ................................................................................................. 15
  Responses to the audit .......................................................................................................... 15

Recommendations ......................................................................................................................... 17

Audit Findings and Conclusions ................................................................................................. 21

1. Introduction ............................................................................................................................. 23
   Objectives of the audit ........................................................................................................ 23
   Context for the audit .......................................................................................................... 24

2. Progress Against the Key Deliverables .................................................................................. 29
   National Automated Fingerprint Identification System (NAFIS) ........................................ 29
   National Criminal Investigation DNA Database (NCIDD) ................................................ 31
   National Child Sex Offender System (NCSOS) .................................................................. 34
   Rapid access to national operational policing data ............................................................. 35
   Controlled access to appropriate information by accredited third parties ...................... 40
   Additional deliverables ...................................................................................................... 44
   Australian Government funding ....................................................................................... 45

3. Achievement of the Broader Objectives of the IGA ............................................................ 47
   Establishment of CrimTrac as a separate agency under the terms of the IGA .............. 47
   Coordinated national policing information systems for a safer Australia ......................... 48
   Framework for timely resolution of key issues .................................................................. 56

4. Project Management ................................................................................................................. 61
   Introduction .......................................................................................................................... 61
   CrimTrac project management methodology .................................................................... 62
   CrimTrac Programme and Project Management Framework issues ................................ 64
   Lack of timely provision of project management skills development .............................. 76

5. IT Security ................................................................................................................................. 78
   Introduction .......................................................................................................................... 78
   The CrimTrac IT environment .......................................................................................... 79
   IT organisational planning ................................................................................................. 80
   IT Security Policy, System Security Plans and procedures .............................................. 84
   Compliance with existing security policies and procedures ........................................... 88
   Clarity of data security roles and responsibilities ............................................................... 93
Appendices

Appendix 1: Survey Form—Views of CrimTrac...........................................................................103
Appendix 2: Survey Form—Views of Police Jurisdictions..........................................................106
Appendix 3: CrimTrac response................................................................................................108
Appendix 4: Special interest party responses .........................................................................114

Index........................................................................................................................................126
Series Titles...............................................................................................................................128
Better Practice Guides.............................................................................................................132
### Abbreviations/Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABCI</td>
<td>Australian Bureau of Criminal Intelligence</td>
</tr>
<tr>
<td>ACSI33</td>
<td>Australian Communications–Electronic Security Instruction 33</td>
</tr>
<tr>
<td>AFIS</td>
<td>Automated Fingerprint Identification System</td>
</tr>
<tr>
<td>AFP</td>
<td>Australian Federal Police</td>
</tr>
<tr>
<td>AGD</td>
<td>Attorney–General’s Department</td>
</tr>
<tr>
<td>ANAO</td>
<td>Australian National Audit Office</td>
</tr>
<tr>
<td>ANCOR</td>
<td>Australian National Child Offender Register</td>
</tr>
<tr>
<td>APMC</td>
<td>Australasian Police Ministers Council—comprising the Ministers who have responsibility for police services in the Commonwealth, States and Territories, and New Zealand.</td>
</tr>
<tr>
<td>ASA</td>
<td>Agency Security Advisor</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>BoM</td>
<td>Board of Management</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CPPMF</td>
<td>CrimTrac Programme and Project Management Framework</td>
</tr>
<tr>
<td>CPRS</td>
<td>CrimTrac Police Reference System</td>
</tr>
<tr>
<td>DCB</td>
<td>Defence Computing Bureau</td>
</tr>
<tr>
<td>DNA</td>
<td>Deoxyribonucleic Acid</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>DSD</td>
<td>Defence Signals Directorate</td>
</tr>
<tr>
<td>DVI</td>
<td>Disaster Victim Identification</td>
</tr>
<tr>
<td>EAMS</td>
<td>External Agency Management System—new system for supporting National Criminal History Record Checking</td>
</tr>
<tr>
<td>EWP</td>
<td>Electronic White Pages</td>
</tr>
<tr>
<td>IGA</td>
<td>Inter–Governmental Agreement</td>
</tr>
<tr>
<td>MNPP</td>
<td>Minimum Nationwide Person Profile</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum / Memoranda of Understanding</td>
</tr>
<tr>
<td>NAFIS</td>
<td>National Automated Fingerprint Identification System</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NCHRC</td>
<td>National Criminal History Record Checking</td>
</tr>
<tr>
<td>NCIDD</td>
<td>National Criminal Investigation DNA Database</td>
</tr>
<tr>
<td>NCSOS</td>
<td>National Child Sex Offender System (now ANCOR)</td>
</tr>
<tr>
<td>NEPI</td>
<td>National Exchange of Police Information</td>
</tr>
<tr>
<td>NEVDIS</td>
<td>National Exchange of Vehicle and Driver Information System</td>
</tr>
<tr>
<td>NFLRS</td>
<td>National Firearms Licence and Registration System</td>
</tr>
<tr>
<td>NHBSS</td>
<td>National Handgun Buyback Support System</td>
</tr>
<tr>
<td>NNI</td>
<td>National Names Index</td>
</tr>
<tr>
<td>NVOI</td>
<td>National Vehicles of Interest</td>
</tr>
<tr>
<td>PANDA</td>
<td>Police Access to National Data Assets</td>
</tr>
<tr>
<td>PBS</td>
<td>Portfolio Budget Statement</td>
</tr>
<tr>
<td>PCC</td>
<td>Project Coordination Committee</td>
</tr>
<tr>
<td>PCPAG</td>
<td>Police Commissioners Policy Advisory Group</td>
</tr>
<tr>
<td>PMO</td>
<td>Project Management Office</td>
</tr>
<tr>
<td>PRS</td>
<td>Police Reference Systems</td>
</tr>
<tr>
<td>PSCC</td>
<td>Protective Security Coordination Centre</td>
</tr>
<tr>
<td>PSM</td>
<td>Protective Security Manual</td>
</tr>
<tr>
<td>SAGEM</td>
<td>Société d’Applications Générales d’Électricité et de Mécanique—the French company chosen to supply the replacement NAFIS. Their role has been extended to maintenance of the system.</td>
</tr>
<tr>
<td>SIG</td>
<td>Strategic Issues Group (a PCPAG proposal)</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SOG</td>
<td>Senior Officers Group of the APMC</td>
</tr>
<tr>
<td>TRA</td>
<td>Threat and Risk Assessment</td>
</tr>
<tr>
<td>UAG</td>
<td>User Advisory Group</td>
</tr>
</tbody>
</table>
Summary and Recommendations
Summary

Background

1. CrimTrac was announced by the Prime Minister in 1998, as a major initiative to help combat crime in Australia through the establishment of a national crime information system.

2. The agency was to replace the National Exchange of Police Information Agreement (the NEPI Agreement) that was established as a National Common Police Service in 1990. CrimTrac ‘contributes to Australian law enforcement through the specification, development, delivery and maintenance of modern, high-quality, rapid access, electronic police information services and investigative tools’.

3. CrimTrac was established through an Inter-Governmental Agreement (IGA) signed by the Australian Government Minister for Justice and Customs and State and Territory Police Ministers, on behalf of their respective governments, on 13 July 2000. CrimTrac was initially an executive agency under the Australian Government Attorney-General’s portfolio. It also became a prescribed agency on 1 July 2002.

4. The Australian Government agreed to ‘host’ the new agency and provided $50 million in one-off funding for the development of new systems. The new systems listed as the key deliverables under the IGA include:

- a new National Automated Fingerprint Identification System (NAFIS);
- a National Criminal Investigation DNA Database (NCIDD);
- a National Child Sex Offender System (NCSOS); and
- rapid access to national operational policing data (CrimTrac Police Reference System (CPRS) Capability Development Programme).

Key findings

Progress against the key deliverables under the IGA (Chapter 2)

5. The ANAO acknowledges that CrimTrac has faced significant challenges in its role of developing and delivering information technology (IT) solutions to service nine\(^1\) police jurisdictions with varying approaches and systems, and with each operating under the constraints of differing Australian Government, State and Territory legislation. In addition to this, CrimTrac has

---

\(^1\) There are nine jurisdictions covering the laws for each State and Territory and the Commonwealth. The ACT Police Services are delivered as an arm of the Australian Federal Police.
continued to deliver and maintain the former NEPI mainframe systems, as well as bringing into place the accountability and reporting mechanisms required to fulfil its obligations as a new Australian Government prescribed agency.

6. CrimTrac has allocated the funding in accordance with the Australian Government’s intentions, but the rate of progress of the key deliverables and, hence, expenditure, has been slower than was originally envisaged. At the time of the audit, some $17.1 million of the $50 million remained unspent. CrimTrac has obtained approval to extend its drawdown of Australian Government monies.

7. NAFIS was delivered early in CrimTrac’s operation. Feedback from the jurisdictions confirms that the system works well, and has enhanced policing operations in this area of forensic science.

8. NCIDD is ‘developed’, but is not yet operationally ‘deployed’. Cross-jurisdictional DNA matching is yet to occur, because of legislative and jurisdictional processes. CrimTrac advised it was hopeful that this will happen by the end of 2003–04 and estimates that over 100 000 profiles will eventually be uploaded. The ANAO acknowledges that the issues leading to the slower than anticipated progress with the NCIDD were due to factors that were not within CrimTrac’s control.

9. The third deliverable, NCSOS, a child sex offender system, was in the concept development stage at the time of the audit. It had been replaced by the concept of a national child protection register, known as the Australian National Child Offender Register (ANCOR) Project, where the jurisdictional registers are centrally hosted at CrimTrac using a common application.

10. Notwithstanding that the new suite of systems to allow rapid access to national policing information, the CPRS Capability Development Programme, was intended for delivery after the NAFIS and NCIDD, progress appears to be slow, and the costs not yet fully determined. The first CPRS system was at a pilot stage with two jurisdictions participating.

11. As well as its identified key deliverables, CrimTrac continues to provide information to accredited third parties under the National Criminal History Record Checking (NCHRC) Programme and has made enhancements to the systems involved in this Programme.

12. The ANAO notes that the IGA did not specify particular timeframes for delivery. However, it was expected that significant progress would be made during the first three years, and that the majority of the funds allocated by the Commonwealth of Australia would be spent within this time.

13. In summary, CrimTrac’s progress in implementing its key deliverables has been variable. One database is fully operational; one system is constructed
but yet to be loaded with all jurisdictions’ data; and two other projects are at the pilot and design phase. CrimTrac has made significant efforts to initiate each of the key deliverables specified in the IGA, with resultant pressures on the resources of the agency.

**Achievement of the broader objectives of the IGA (Chapter 3)**

14. The ANAO considered the strategic and operational context of the agency. The police jurisdictions, as well as being the users of the CrimTrac systems, are also partners under the IGA and, as such, are also involved in the design and development of the projects and systems. The various jurisdictions provide a significant source of the funding for CrimTrac’s operations.

15. The ANAO concluded that the establishment of CrimTrac as an Australian Government agency has resulted in the alleviation of many of the issues of its predecessor, NEPI. Although progress in some projects has been slower than anticipated, CrimTrac has progressed the key deliverables; implemented many internal plans and controls; and has continued to provide support for the former PRS systems.

16. However, the ANAO concluded that there would be benefit in CrimTrac seeking to better define the links between the broad objectives of the IGA and its Outcome, which is ‘Coordinated national policing information systems for a safer Australia’.

This would provide an increased understanding of the context of the CrimTrac projects and a common goal for all parties to work towards.

17. The ANAO also considered that it is difficult for CrimTrac to measure and report against its stated Outcome. However, the ANAO further considered there would be benefit in CrimTrac, in consultation with its partners, seeking the means to better reflect what is collectively being achieved, which would benefit both efficient and effective management and enhanced external accountability.

18. The ANAO also found that the IGA has limitations with respect to the partnership approach. We concluded that there would be benefit for the arrangement by establishing a formal agreement, such as a Memorandum of Understanding (MOU), between all the partners, as the basis for setting out the expected responsibilities of each partner in their role as a signatory to the IGA.

19. The deployment of the deliverables under the objectives of the IGA, and hence the achievement of the CrimTrac Outcome, are likely to continue to be subject to legislative amendment issues, such as those impeding the deployment of NCIDD. The ANAO recommended that CrimTrac consult with

its key external stakeholders to develop a framework that allows for the timely resolution of key issues that pose a risk to the CrimTrac Outcome, or to particular projects.

**Project management (Chapter 4)**

20. CrimTrac had a sound project management methodology in place in PRINCE2. This methodology was adapted to develop an in-house project management framework, the CrimTrac Project and Programme Management Framework (CPPMF). However, there were some weaknesses in the manner of adaptation and implementation of the CPPMF, leading to difficulty in tracking the history of projects, and some difficulties in the coordination of projects. CrimTrac had already taken some steps to rectify these. During the audit, the agency commissioned a consultant to examine a current project, and to consider whether changes were required in the overarching project management framework.

21. The ANAO concluded that the agency’s project management framework is not sufficiently robust to be effective in a multi-agency project delivery environment. The ANAO made recommendations aimed at strengthening the framework through: providing more detailed policy and guidance; measuring the full costs and benefits of projects; better detailing the roles and responsibilities of all parties and how they should interact; and establishing an arrangement to more effectively coordinate the projects.

**Data and IT security (Chapter 5)**

22. The ANAO has reported a number of findings relating to the controls and procedures in place to ensure the security of CrimTrac’s systems, as well as the security of data it either holds, or accesses, for matching purposes. The ANAO notes that most of CrimTrac’s data is only accessible by police jurisdictions and that, to date, there have been no security breaches or incidents of significance. However, as CrimTrac continues to build systems and to host increasing volumes of sensitive data, it is important that adequate controls are in place to protect the data.

23. The ANAO found that, although the existing CrimTrac Security Policy was generally compliant with the Protective Security Manual, the links to appropriate TRAs were insufficiently established. As a consequence, the procedural environment to ensure the protection of data was weakened. CrimTrac would benefit from finalising the development of its various IT security plans, policies and procedures, as well as implementing measures to ensure greater consistency between these plans. This would minimise the risks of gaps in the agency’s approach to the management of the security of its data and systems. The ANAO considers that CrimTrac should finalise its IT Strategic Plan, Business Continuity Plan and Disaster Recovery Plan.
24. The ANAO further concluded that CrimTrac should take action to: establish formal agreements with the jurisdictions which cover the ownership of the data and systems, and assign responsibilities for the security of these data and systems accordingly; ensure that its formal agreements with its service providers are up to date, finalised and appropriately signed off; and take a more strategic approach to the security training of staff and users of its various systems.

**Overall audit conclusion**

25. CrimTrac has faced significant challenges in its role of developing and delivering IT solutions to service Australia’s police, as well as maintaining the former NEPI mainframe systems, and establishing itself as a new Australian Government executive and prescribed agency. Although progress in delivering the key deliverables under the IGA has been variable, the CrimTrac agency has exerted significant effort to initiate all of the deliverables, and appears to have successfully replaced its predecessor, NEPI.

26. The ANAO concluded that, after some three years of operation, it is timely for a review of the nature of the relationship between the partners in the CrimTrac initiative, and a clarification of their various roles and responsibilities. The ANAO considered that better definition of the links between the broader objectives in the IGA and the CrimTrac Outcome would be useful in providing a common goal for all parties to work towards.

27. The ANAO also concluded that more work needed to be done to: refine CrimTrac’s strategic monitoring of its projects; provide more detailed guidance to project managers; and clarify the role of CrimTrac as the coordinating agency as well as the responsibilities of jurisdictions as project partners.

28. There is also significant scope to enhance the controls and procedures in place to ensure the security of CrimTrac’s systems, as well as the security of data it either holds, or accesses, for matching purposes. As CrimTrac continues to build systems and to host increasing volumes of sensitive data, it is important that adequate controls are in place to protect the data.

**Responses to the audit**

**Agency response**

29. CrimTrac has agreed with all of the recommendations, and provided its response to the audit as follows:

The CrimTrac initiative’s primary challenge has been to gain co-operation—financial and technical across 9 disparate police services—then give police nationwide access to centrally hosted information technology tools and services that support each jurisdiction’s approach plus introduce new
nationwide capabilities not addressed by the former NEPI. This has required a significant personal investment by Agency staff in creating and maintaining effective jurisdictional relationships since the Agency was created in 2000.

CrimTrac’s programmes being delivered under the IGA strive for consensus and trust with and between police jurisdictions before they are designed and implemented. It takes time, however,—much more time than the original CrimTrac proponents contemplated and whilst a slower than optimum rate has been observed by the audit, responsible spending and prudential management of the Australian Government’s $50 million investment has been demonstrated.

Weaknesses reported in project management and data security had already received the attention of the CrimTrac Board of Management prior to notification of the audit. Through the Agency’s risk management approach, they were identified as high priority areas for attention and significant resources were allocated to improve outcomes in these areas. The risk exposure as it currently stands is understood by all stakeholders as the Agency continues to mitigate it.

The Agency is refining its role and modus operandi within the stakeholder arrangements of the CrimTrac initiative and the stakeholders are refining their understanding of how best to participate in and exploit the opportunities that CrimTrac provides. The audit has been a valuable opportunity to take stock of our progress and to note constructive criticism that should strengthen the Agency in its contributions to improved community safety.

30. The full agency response is included at Appendix 3.

Special interest party responses

31. The ANAO also sought comments from the police jurisdictions and the Attorney-General’s Department (AGD) as special interest parties, and these are detailed in full in Appendix 4. In summary, the police jurisdictions and the AGD were supportive of the report and its recommendations.
Recommendations

Set out below are the ANAO’s recommendations, with abbreviated responses from CrimTrac. Where CrimTrac has provided a more detailed response, this is shown in the body of the report, immediately after each recommendation. The ANAO considers that priority should be given to recommendations 1, 5, 6, 7 and 9.

Recommendation No.1
Para 3.39
Clarify roles and responsibilities

The ANAO recommends that, to supplement the Inter-Governmental Agreement, CrimTrac seek to establish a formal agreement between all the partners that clearly defines the agreed roles and responsibilities of each partner.

Agency response: Agree.

Recommendation No.2
Para 3.78
Develop a framework for resolution of key issues

The ANAO recommends that CrimTrac consult with its key stakeholders to develop a framework for the timely resolution of key issues that pose a risk to the CrimTrac Outcome or to particular projects.

Agency response: Agree.

Recommendation No.3
Para 4.43
Strengthen project management

The ANAO recommends that CrimTrac strengthen its project management approach through enhancing its CrimTrac Programme and Project Management Framework by:

a) providing supporting policies and more detailed procedural guidance to programme and project managers; and

b) measuring and/or assessing the full costs and benefits of its projects.

Agency response: Agree.
Recommendation No.4
Para 4.67
Define project management roles and responsibilities
The ANAO recommends that CrimTrac more clearly define, and set out in its overall project management framework, the roles and responsibilities of both the agency and jurisdiction project managers, including how the parties are to interact in order to progress the projects efficiently and effectively.

Agency response: Agree.

Recommendation No.5
Para 4.84
Coordinate projects
The ANAO recommends that CrimTrac establish an arrangement to more effectively coordinate its projects in a transparent and accountable manner.

Agency response: Agree.

Recommendation No.6
Para 5.28
Develop BCP and DRP
The ANAO recommends that CrimTrac develop its Business Continuity Plan and Disaster Recovery Plan and accompanying procedures.

Agency response: Agree.

Recommendation No.7
Para 5.40
Develop IT plans
The ANAO recommends that CrimTrac establish an IT Strategic Plan that addresses, plans and coordinates the use of IT as a foundation to support all CrimTrac’s business objectives. The IT Strategic Plan should be complemented by appropriate IT operational and business plans.

Agency response: Agree.
Recommendation No.8
Para 5.83
Integrated data security

The ANAO recommends that CrimTrac, in consultation with its partners under the Inter-Governmental Agreement, develop an integrated approach to the management of data and system security across the agency. The approach should include developing:

a) the full set of system security plans; and

b) monitoring and evaluation mechanisms to ensure the compliance of each system and its users with the specified system security procedures.

Agency response: Agree.

Recommendation No.9
Para 5.104
Assign data security responsibility

The ANAO recommends, for the purposes of maintaining consistency of data security, that CrimTrac seek to establish Memoranda of Understanding with the jurisdictions that agree the security standards to be applied and assign responsibility for monitoring compliance.

Agency response: Agree.

Recommendation No.10
Para 5.115
Review and finalise agreements

The ANAO recommends that CrimTrac review its formal agreements with its service providers to make sure that these agreements are up to date, finalised and appropriately signed off.

Agency response: Agree.

Recommendation No.11
Para 5.129
Security training

The ANAO recommends that CrimTrac review its security training policies and procedures and develop a strategic approach to the training of all those involved in the development, management, support or use of its various systems.

Agency response: Agree.
Audit Findings and Conclusions
1. Introduction

This chapter outlines the audit objectives and provides the context for the audit.

Objectives of the audit

1.1 The overall objective of the audit was to assess CrimTrac’s progress in achieving the key deliverables it was established to provide, given that the agency had been in operation for some three years. The Australian Government provided $50 million for the implementation of CrimTrac, with an expectation that significant progress would be made within the first three years. The audit further examined whether CrimTrac had progressed the key deliverables efficiently and effectively.

1.2 To this end, the audit criteria focused on the following:

- CrimTrac’s progress in achieving the key deliverables identified in the Inter-Governmental Agreement (IGA) in accordance with the agreed order of delivery (Chapter 2);

- CrimTrac’s progress in achieving the broader objectives of the IGA (Chapter 3);

- whether CrimTrac had planned and managed the projects to deliver them efficiently and effectively (Chapter 4); and

- whether the data either held by CrimTrac, or accessed through CrimTrac, for matching purposes is secure (Chapter 5).

Audit methodology

1.3 The audit methodology included:

- interviewing CrimTrac executives and programme/project managers;

- examining key CrimTrac corporate documents and information, including the Inter-Governmental Agreement, the Charter of Governance, CrimTrac Strategic Plan 2001–05, Annual Reports for 2001–02 and 2002–03 as well as various corporate policies such as those relating to security, risk management, internal audit and privacy of information;

- holding discussions with relevant staff from the Office of the Federal Privacy Commissioner, the Commonwealth Ombudsman’s Office and the Attorney General’s Department;
• tracking of the key deliverables through the minutes from the Board of Management meetings, the Project Coordination Committee meetings and selected User Advisory Group meetings;

• inviting CrimTrac to participate in a survey to seek the agency’s views on its performance in achieving the key deliverables, the challenges presented and how it had managed these, including any lessons learned (Appendix 1);

• inviting the nine police jurisdictions to participate in a survey to seek their views on the performance of CrimTrac in achieving the key deliverables, the challenges presented, how well these had been managed by the agency, and jurisdictions’ views on CrimTrac’s role for the present and the future (Appendix 2);

• visiting two jurisdictions to hold direct discussions on the implementation process;

• reviewing CrimTrac’s IT security policies/procedures; and

• testing the application of the IT policies and procedures, mainly for the National Automated Fingerprint Identification System (NAFIS) and the National Criminal Investigation DNA Database (NCIDDD).

1.4 The team engaged two specialist IT auditors to assist in the assessment of CrimTrac’s data and system security policies and to test how well these were being applied in practice, as well as the extent of monitoring of compliance.

1.5 The audit was conducted in conformance with ANAO auditing standards and cost $305,000.

Context for the audit

The establishment of CrimTrac

1.6 CrimTrac was announced by the Prime Minister in 1998, as a major initiative to help combat crime in Australia through the establishment of a national crime information system. The main bases for the decision were the need to replace the National Automated Fingerprint Identification System (NAFIS), to take advantage of the major gains possible from using DNA as evidence, and to help fight the increasing mobility of criminal activity.

1.7 The CrimTrac agency replaced the National Exchange of Police Information (the NEPI) that was established by an Inter-Governmental Agreement as a National Common Police Service in 1990. In 1998, the Australasian Police Ministers Council (APMC) resolved to support the Australian Government’s proposal to provide a central infrastructure for
national law enforcement systems. In 1999, the APMC noted the proposed governance model for CrimTrac and agreed to establish the IGA.

1.8 CrimTrac was established in July 2000 through an IGA signed by the Australian Government Minister for Justice and Customs and State and Territory Police Ministers on behalf of their respective governments. CrimTrac was initially an executive agency under the Australian Government Attorney-General’s portfolio. It remains an executive agency, and also became a prescribed agency on 1 July 2002. CrimTrac’s vision, as stated in its 2002–03 Annual Report, is: ‘to be a regional and world leader in the development, implementation and management of advanced information systems that assist police nationally in their law enforcement and crime prevention roles’.

1.9 The Australian Government agreed to ‘host’ the new agency due to the perceived difficulties with the NEPI model. Under the NEPI model, insufficient funds were put aside to replace the NAFIS, which was predicted to become unserviceable by early 2001.

1.10 In establishing the CrimTrac agency as an Australian Government entity, it was agreed that the imperatives of better reporting and accountability, as well as more transparent and more effective funds management, would be included. It was also determined that there would be a Board of Management (BoM) instead of a Board of Control. A project office was established in the Australian Government Attorney-General’s Department (AGD) to draw up the blueprint for the new agency.

The objectives and key deliverables of CrimTrac

1.11 Under the recitals of the IGA it was specified that CrimTrac would, in the coming years, include the following key deliverables:

- a new National Automated Fingerprint Identification System (NAFIS);
- a National DNA Criminal Investigation System (now titled NCIDD);
- a National Child Sex Offender System (NCSOS); and
- the provision of rapid access to national operational policing data.\(^3\)

1.12 Under the IGA, the CrimTrac framework is intended to provide the means by which these components, and other emerging policing requirements across jurisdictions, can be considered and met as appropriate.

1.13 Additionally, one of CrimTrac’s business deliverables is to ‘provide controlled access to appropriate information by duly accredited third parties’.\(^4\)

---

\(^3\) Inter-Governmental Agreement, For the establishment and operation of ‘CrimTrac’, a national law enforcement information system for Australia’s Police Services. 13 July 2000. Recital D, p.2.

\(^4\) ibid. p.6.
This is done by the National Criminal History Record Checking Programme (NCHRC), which is a continuation of the NEPI function.

1.14 CrimTrac is also to provide support for the jurisdictions in the implementation and use of its services.

**Roles and responsibilities under the IGA**

1.15 The IGA endeavours to outline the roles and responsibilities of the parties involved in the CrimTrac initiative. These are described further in CrimTrac’s Charter of Governance.

1.16 Under the IGA, the role of the APMC is to:

- consider the high level strategic and policy directions for CrimTrac;
- approve the agency’s Strategic Plan;
- approve any new initiatives requiring special funding or changes to legislation; and
- consider and approve the appointment of members to the Board of Management.

1.17 The Senior Officers Group (SOG), as the advisory body to the APMC for policing issues, advises on CrimTrac matters and approves the two non-voting members of the BoM.

1.18 The CrimTrac BoM is responsible and accountable for the efficient and effective delivery of the CrimTrac initiative. The BoM is comprised of one voting Australian Government member (since inception this has been a Deputy Secretary from AGD), two voting members from large jurisdictions and two voting members from small jurisdictions, as well as two non-voting members to provide specialist advice in the areas of IT and finance. The IGA specifies that BoM members are to act in good faith, and are to act in the interests of nationwide policing and the CrimTrac initiative.

1.19 The IGA provided for the inaugural Chairperson to be the Australian Government representative, in recognition of the $50 million capital contribution made by the Australian Government. The Australian Government representative has the power of veto over the $50 million contribution.

1.20 The IGA provides for the appointment of a Chief Executive Officer (CEO), who is responsible to the BoM for the effective delivery of services as well as for the day-to-day management of the agency.

---

5 The large jurisdictions are NSW, Vic, and Qld; the small jurisdictions are WA, SA, NT, Tas, and the ACT. BoM membership is rotated at the determination of the APMC, although members are generally appointed for a term of three years.
1.21 The role of police jurisdictions is not defined in the IGA. However, Clause 3.2 specifies that ‘the parties agree to cooperate fully with each other to develop and deliver the objectives of CrimTrac’.

### Operating costs and funding arrangements

1.22 The Australian Government agreed to provide $50 million, on a one-off basis, for the implementation of the CrimTrac agency and the initiation of the key deliverables. The figure was derived from an estimate of $30 million to replace the failing fingerprint system, NAFIS, and a further $20 million for new systems.

1.23 Documents examined by the ANAO, and early budget proposals, suggested it was envisaged this money would be expended within the first three years of operation, notionally at a rate of $20 million in each of the first two years of operation and $10 million in the third year.

1.24 The AGD advised the ANAO that the Australian Government did not intend to compel jurisdictions to participate in all CrimTrac projects. Rather, police jurisdictions should participate in those projects considered to be of benefit to them. However, the Australian Government anticipated that most jurisdictions would, in the end, participate in most projects in the interests of nationwide policing, and because choosing not to participate would become a disadvantage.

1.25 The Australian Government monies have been used largely for project development costs, with ongoing systems being funded by the contributions from the jurisdictions by way of annual subscriptions based on recognised police strength. The agency also generates fee revenue from criminal history checks under the NCHRC Programme.

1.26 Under the IGA Clause 3.2, jurisdictions that choose to participate in a CrimTrac project must ‘meet the costs of that project in a manner which is equitable and agreed to by all participating jurisdictions’.

1.27 This Clause further states that the benefits, costs and risks must be transparent to each jurisdiction, and that CrimTrac is to be conducted in accordance with sound business principles and high standards of financial accountability.

1.28 Jurisdictions may also agree to provide funds for CrimTrac projects of particular interest to them. Any work required to change systems in the jurisdictions to make them compatible with the new CrimTrac systems is funded and resourced by the jurisdictions.
1.29 During 2002–03 CrimTrac employed 39 ongoing staff plus 3 non-ongoing staff, and supplemented them with some 20 contractors, who were all based in Canberra.

Additional deliverables

1.30 CrimTrac has also achieved deliverables in addition to those identified in the IGA. These include the Disaster Victim Identification (DVI) Tool used after the bombing in Bali in October 2002, and the National Handgun Buyback Support System (NHBSS), established in 2003 at the Australian Government’s request. CrimTrac received an additional $2.7 million in Australian Government funds for the NHBSS Project, drawn down over 2002–03 and 2003–04.

---

2. Progress Against the Key Deliverables

This chapter examines CrimTrac’s progress against the key deliverables identified in the IGA in accordance with the agreed order of delivery and subsequently established milestones.

2.1 The key deliverables under the recitals of the IGA are:

- a new National Automated Fingerprint Identification System (NAFIS);
- a National DNA Criminal Investigation System (now titled NCIDD);
- a National Child Sex Offender System (NCSOS); and
- the provision of rapid access to national operational policing data (CPRS Capability Development Programme).

2.2 It was understood by the IGA partners that the systems were to be delivered in the above order of priority and that significant progress would be made within three years.

2.3 Additionally, CrimTrac was to maintain the existing NEPI systems (Police Reference Systems) and to provide controlled access to appropriate information by duly accredited third parties. This is done by the National Criminal History Record Checking Programme (NCHRC), which is also a continuation of a NEPI function.

2.4 CrimTrac’s progress against each of these key deliverables is addressed below.

National Automated Fingerprint Identification System (NAFIS)

2.5 CrimTrac was to replace the failing NEPI fingerprint system with a modern, sustainable system. The new NAFIS was the first system to be delivered. It was developed within the notionally allocated budget of $22 million, and it became operational in April 2001. A French company, SAGEM, developed NAFIS and continues to provide the support and maintenance for the system.

2.6 NAFIS is a computerised fingerprint and palm database that stores and matches fingerprint and palm print records obtained by police jurisdictions. It is used by law enforcement agencies as a means to positively identify a person.

---

7 op. cit. Inter-Governmental Agreement, Recital D. p.2.
of interest to police, and to help solve major and minor crimes. Although the initial matching is conducted by the NAFIS system, the ANAO was advised that an accredited fingerprint expert always confirms the match manually. CrimTrac is exploring options for ‘lights out’ processing, whereby the manual confirmation would be minimised.

2.7 The NAFIS contribution to the CrimTrac Outcome, as described in the CrimTrac Annual Report 2002–03, is: ‘NAFIS assists police in establishing identity from fingerprints and palm impressions more quickly and reliably and contributes to the solving of crime’. The report states that NAFIS stores some 2.8 million fingerprints and some 5.4 million palm impressions as well as 462 000 latent prints from unsolved crime scenes.

2.8 On average, 12 500 crime scene latent searches are conducted on NAFIS each month, comprising some 11 000 fingerprints and some 1500 palm impressions, with 10 per cent resulting in an identification.

2.9 The Annual Report further states that: ‘NAFIS incorporates the largest electronic palm database in the world. The matching results achieved against the palm database have significantly improved the ability of police to resolve volume and major crimes across Australia’.

2.10 In establishing the new NAFIS, CrimTrac overcame some significant challenges, such as extensive contract management negotiations with SAGEM, and the conversion of the existing data previously captured in the former NEPI fingerprint system. The latter was done offshore at a SAGEM facility in Tacoma, USA. CrimTrac advised that Australian police supervised the shipment of fingerprint records to, and from, the conversion facility. SAGEM are contracted to provide maintenance and support of the system until April 2004 and, after that, on an ongoing annual contract extension basis.

2.11 It was evident to the ANAO that CrimTrac considers NAFIS to be a success, a view that was supported by the jurisdictions in their responses to the ANAO survey.

**NAFIS workstations and Livescan devices**

2.12 In addition to developing the new NAFIS, CrimTrac encouraged jurisdictions to make best use of emerging forensic technologies.

2.13 CrimTrac supported jurisdictions in their adoption of Livescan technology, whereby finger and palm prints are recorded by laser scanning rather than by the traditional ink and roller method. The quality of the resultant images is superior. The speed of taking the prints and the automated

---

9 ibid. p.15.
uploading into NAFIS allows for the rapid identification of persons of interest at the time of their arrest.

2.14 As at March 2004, there were some 94 Livescan devices integrated with the CrimTrac NAFIS, with a further 50 devices planned to come on line.\(^\text{10}\)

2.15 The ANAO notes that NAFIS has already received an upgrade, costing some $5.6 million, in early 2003.\(^\text{11}\) This used the balance of the original allocation for NAFIS, plus some $2.8 million that was notionally allocated to the CPRS Capability Development Programme. CrimTrac advised that the upgrade was required due to greater usage than was envisaged, arising from the increased speed and ease of use, and in part relating to the removal of the users’ transaction fee.

2.16 CrimTrac further advised that the NAFIS handles approximately double the throughput of the former NEPI system, and it now has sufficient capacity for the next three years.

**Conclusion on the status of NAFIS**

2.17 The ANAO concluded that CrimTrac managed the delivery of the new NAFIS well. The system was delivered early in CrimTrac’s operation and was achieved within the notional budget allocation. Feedback from the jurisdictions confirms that the system works well and has enhanced policing operations in this area of forensic science.

2.18 The ANAO also concluded that CrimTrac and the jurisdictions have made good use of technology in adopting the Livescan devices and in encouraging their uptake.

**National Criminal Investigation DNA Database (NCIDD)**

2.19 The National Criminal Investigation DNA Database (NCIDD) is intended to provide all Australian police services with the capability to conduct cross-jurisdictional DNA profile matching within one system. NCIDD will allow the matching of profiles within jurisdictions and across jurisdictions, in accordance with relevant legislation.

2.20 The Annual Report for 2002–03 defines the contribution of this system to the CrimTrac Outcome in the following terms: ‘The NCIDD assists police in establishing identity more quickly and reliably from human biological samples and contributes to the solving of crime’.

\(^{10}\) ibid. p.19.

\(^{11}\) ibid. p.19.
The NCIDD Output is the: ‘development, deployment and maintenance of a national DNA database that will automatically accept, store and match DNA profiles from every Australian police jurisdiction’.

The NCIDD was developed in two parts: a central database and matching engine; and the component to integrate the database with an automated jurisdictional laboratory information management system.

In CrimTrac’s view, the system has been ‘delivered’, since the development of the central database and matching engine was completed on 20 June 2001. The trial and provision of the laboratory information management system to the participating jurisdictions was completed in March 2003. According to the CrimTrac Annual Report 2002–03, it is the only DNA database using web technology with an online entry system in the world. Users can search results instantly via a secure web browser linked to the central database at CrimTrac.

However, at the time of the audit, only DNA profiles from NSW and QLD had been loaded into NCIDD. The ANAO was advised that CrimTrac expected to load profiles from Victoria in early 2004, and that profiles from most other States and Territories should be loaded in the first half of 2004. At the time of the audit, no cross-jurisdictional matching had occurred.

Legislative issues

The ANAO was advised that the delays in the deployment of NCIDD were due to the need for all States and Territories to make legislative changes to ensure that DNA matching occurred, as provided for under the provisions of the Commonwealth Crimes Act 1914 (as amended).

Each DNA profile on NCIDD must be associated with an index as set out in legislation—for example: crime scene; offender; and suspect or volunteer. Each index attracts a set of rules surrounding destruction provisions, matching provisions and identification provisions. The NCIDD database is designed to ensure that only those links complying with the legislative matching requirements are available for the users to view. To do this, the system requires a complex matching matrix to be encoded into the programme.

Before the matrix can be encoded: the legislative provisions in each State and Territory must be amended to allow for the matching to occur; Memoranda of Understanding (MOU) must be signed between CrimTrac and each jurisdiction; and administrative arrangements must be in place between each of the jurisdictions. Table 2.1 shows the status of the preparation and signing of these MOU, Ministerial Arrangements, and Matching Tables as at January 2004.
Table 2.1
Jurisdictional legal status to allow NCIDD participation—as at 23 January 2004

<table>
<thead>
<tr>
<th></th>
<th>Number to be completed</th>
<th>Completed</th>
<th>In progress</th>
<th>Per cent completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOU with CrimTrac</td>
<td>9</td>
<td>4</td>
<td>5</td>
<td>44</td>
</tr>
<tr>
<td>Ministerial Arrangement</td>
<td>72</td>
<td>16</td>
<td>56</td>
<td>22</td>
</tr>
<tr>
<td>Cross-jurisdictional Matching Table</td>
<td>72</td>
<td>1</td>
<td>71</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: ANAO analysis of CrimTrac data.

CrimTrac’s efforts to progress the legislative issues

2.28 CrimTrac has faced considerable challenges in attempting to facilitate the progress of the legislative amendments. The main responsibility for the negotiations with State and Territory governments, and the State Attorneys-General, has been undertaken by the Australian Government AGD, which has responsibility for legislative reform. The ANAO was advised by CrimTrac, the AGD, and the jurisdictions, that CrimTrac should not be held solely accountable for the slow progress in the legislative reform.

2.29 Nonetheless, CrimTrac had made efforts to monitor the progress of the legislative changes. The ANAO considers that these efforts might have been better supported by appropriate and timely raising of the issue with key stakeholders, in order to seek the assignment of priority to the legislative changes required in each State and Territory, and by the Commonwealth of Australia.

Conclusion on the status of NCIDD

2.30 The ANAO concluded that, although the system can be described as having been ‘developed’, it has not yet been fully operationally ‘deployed’. Although some States have loaded profiles, it does not yet automatically accept, store and match DNA profiles within and across every Australian police jurisdiction. CrimTrac advised it was hopeful that this will occur by the end of 2003–04, and estimates that over 100 000 profiles will eventually be uploaded.

2.31 The ANAO acknowledges that the issues leading to the slower than anticipated progress with the NCIDD were due to factors that were not directly within CrimTrac’s control. The ANAO concluded that CrimTrac would benefit from a clarification of the roles and responsibilities with respect
to the management of legislative issues that impact upon CrimTrac’s business, as well as the establishment of a formal framework through which key issues can be raised with stakeholders, and a timely resolution sought. This is addressed in detail in Chapter Three.

**National Child Sex Offender System (NCSOS)**

2.32 The NCSOS was listed as the third key deliverable in the IGA, to be developed after the new NAFIS and the DNA database.

2.33 This project was initially viewed as a system to facilitate the rapid and efficient nationwide sharing of jurisdictionally endorsed information on child sex offenders and suspects between police jurisdictions. The project was formally initiated in June 2002. It planned to focus on the exchange of factual information first, and then to consider mechanisms to link with the Australian Crime Commission intelligence holdings. In this way, employment-screening processes could be improved by a combined use of intelligence and factual information—to the extent possible given the constraints on the use of non-factual data.

2.34 Early attempts to initiate this project were delayed by discussions on the feasibility of using non-factual information. Jurisdictions expressed concern about the untested nature of such information and indicated a preference for restricting the system to factual data.

2.35 CrimTrac advised that there were also insufficient staffing resources in the CPRS Capability Development Programme team to progress this project, as well as the other CPRS Capability Development Projects that were already in varying conceptual stages.

2.36 In the meantime, in 2000, the NSW Police Service had implemented a Child Protection Register with reporting requirements. CrimTrac advised that NSW considers that this register had proved to be an effective tool for the case management of convicted child sex offenders. As an indicator, numerous offenders had been reported by NSW Police as having moved interstate, where there were no corresponding laws or registers.

2.37 In November 2002, the APMC approved the establishment of an inter-jurisdictional working party/police commissioners policy advisory group, including CrimTrac and the then Australian Bureau of Criminal Intelligence, to develop a proposal for a nationally consistent approach for the monitoring of convicted child sex offenders.

2.38 In accordance with CrimTrac’s charter to adopt a ‘best-of-breed’ approach where desirable and practicable, the NCSOS Project subsequently changed focus to consider the implementation of a National Child Protection Register along the lines of the NSW system. The proposed system was labelled
the Australian National Child Offender Register (ANCOR). The APMC approved the project in November 2003 and further resolved that it should be delivered by 1 July 2004.

2.39 The APMC has approved the project in November 2003 and further resolved that it should be delivered by 1 July 2004.

ANCOR has been funded two-thirds by the jurisdictions and one-third by the Australian Government, using a combination of $1 million from the $50 million capital injection and the remainder by additional funds from the Australian Government and the States and Territories.

2.41 CrimTrac presented a design concept to the APMC in November 2003 that was well received. In the jurisdictions’ responses to the ANAO survey, the majority of jurisdictions indicated a high degree of support for the APMC Project. Some expressed concern that the tight timetable set by the APMC may lead to an early need to revise the system once it has become operational. Some expressed further concern that the required legislation was not yet in place to ensure the data sharing could lawfully occur. CrimTrac advised that ANCOR is now scheduled for delivery in September 2004, in part due to legislative amendments.

Conclusion on the status of NCSOS

2.42 The APMC concluded that NCSOS, replaced by the ANCOR Project, was in the concept development stage at the time of the audit.

2.43 The APMC also concluded that the deadline imposed by the APMC should ensure the timely completion of this project as well as timely jurisdiction responses and support. However, the APMC also notes that some elements of ANCOR are reliant on developments in other CrimTrac projects and initiatives, such as the Common Information Model, the data dictionary, and some of the Common Services Project. It will be important that these projects are well coordinated at the strategic level.

Rapid access to national operational policing data

2.44 The fourth key deliverable under the Recitals of the IGA is ‘the provision of rapid access to national operational policing data’. Under Clause 10.2, this is described as ‘integrated police access to national operational policing data’.
2.45 The Police Reference Systems (PRS) existed as mainframe systems under NEPI. At the time that NEPI was wound down, the need to update and better integrate these systems had already been identified and the Police Access to National Data Assets (PANDA) concept was devised.

2.46 When CrimTrac took over the NEPI functions in July 2000, it inherited the existing systems as well as the PANDA concept.

The existing mainframe systems—the PRS

2.47 The existing PRS consists of a range of former NEPI mainframe systems that provided information to operational police and accredited agencies. CrimTrac maintains these mainframe systems and continues to provide access to the information to the jurisdictions.

2.48 The current mainframe systems include the:

- National Names Index (NNI);
- National Firearms Licensing and Registration System (the NFLRS);
- National Vehicles of Interest (the NVOI);
- The AUSTROADS National Exchange of Vehicle and Driver Identification System (NEVDIS);
- The TELSTRA Electronic White Pages (EWP); and
- Online Telephone Directory (OTD).

2.49 These systems are considered by CrimTrac to be an ongoing business deliverable, and are fully funded by the jurisdictions. CrimTrac’s Annual Report 2002–03 describes the PRS contribution to its Outcome in the following terms: ‘Coordinated national policing information systems for a safer Australia’. The PRS Output is ‘the provision of national access through the maintenance of the systems’.

2.50 Access to these systems is restricted to police and authorised non-police law enforcement agencies, such as the Australian Crime Commission and the Australian Customs Service, which may only access the specific data required.

2.51 CrimTrac made a strategic decision that these systems would not be improved in the mainframe environment but would, instead, be migrated to midrange computing platforms as part of the CPRS Capability Development Programme.\(^{12}\) CrimTrac envisaged that the mainframe systems would be decommissioned within the first three years of the agency’s operation.

---

\(^{12}\) However, in December 2002, CrimTrac arranged for the mainframe system to be moved from the Defence Computing Bureau (DCB) at Victoria Barracks to the DCB in Canberra, which provided a more modern mainframe environment and enhanced system capacity and performance.
2.52 The current systems allow each jurisdiction to query across other jurisdictions’ data, but the systems are designed as ‘stovepipes’. This means that an officer wanting information on a particular person, or vehicle, may have to query the NNI, the NVOI, and the NFLRS in order to ascertain sufficient details regarding the person; whether the vehicle being driven is of interest; and whether the person was likely to be armed.

2.53 The rate of usage of these systems remains high, and in some cases has increased from the previous NEPI usage rates because of increased capacities.

**Table 2.2**

**Usage of the PRS systems 2001–02 and 2002–2003**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NNI</td>
<td>3.70 million</td>
<td>4.36 million</td>
<td>+29</td>
</tr>
<tr>
<td>NFLRS</td>
<td>74 808</td>
<td>82 836</td>
<td>+11</td>
</tr>
<tr>
<td>NVOI (new incidences)</td>
<td>250 824</td>
<td>206 322</td>
<td>−18</td>
</tr>
<tr>
<td>OTD</td>
<td>112 596</td>
<td>97 104</td>
<td>−14</td>
</tr>
<tr>
<td>EWP charges</td>
<td>$387 828</td>
<td>$342 384</td>
<td>−12</td>
</tr>
</tbody>
</table>


2.54 The cost of maintaining these systems was $1.8 million in 2002–03.

2.55 The ANAO notes that it is costly for a small agency such as CrimTrac to maintain and support two IT environments. The ANAO considers that not only would it be in line with better practice to move to one operating platform, it would also result in a positive impact on the operational costs and effectiveness of CrimTrac, including efficiency savings for police jurisdictions in querying integrated and improved systems.

**Conclusion on the status of the PRS systems**

2.56 The ANAO concluded that CrimTrac continues to deliver these mainframe systems in accordance with police requirements. However, the envisaged decommissioning of the systems after three years is behind schedule. There is not yet a date determined for this to occur. This is due to the slower progress of the replacement systems under the CPRS Capability Development Programme, and is also attributable to the differing stages of IT development in the jurisdictions, with some not yet able to provide a web-based interface to the PRS.
The future systems—the CPRS Capability Development Programme

2.57 The Police Access to National Data Assets (PANDA) Project was renamed the CPRS Capability Development Programme (hereafter referred to as the CPRS).

2.58 Under the CPRS, CrimTrac will modernise and improve the PRS systems and develop further systems. CrimTrac proposes to move the existing systems from a mainframe platform to midrange platforms. The end result will be a suite of integrated systems that delivers comprehensive data to police.

2.59 The change from the example cited above, in paragraph 2.52, is that a police officer will be able to conduct a single online query from a police patrol car, or via a hand held wireless data device, to determine whether the person is known in any jurisdiction to be:

- a threat to police safety;
- a threat to themselves or others;
- of interest to police; and/or wanted by police; and
- whether the vehicle is of interest.

2.60 In CrimTrac’s Annual Report 2002–03, the contribution to the CrimTrac Outcome is described as: ‘CPRS redevelopment contributes to rapid, efficient and cost-effective access to operational policing information and information-related services required by police nationwide in the performance of their duties and for their improved safety’.\(^\text{13}\)

2.61 CrimTrac considers that CPRS also meets the requirement, under the IGA, for the agency to consider and develop new capacities to meet the emerging policing requirements across jurisdictions as appropriate.

2.62 The initial notional budget allocation for CPRS was $22 million. At the time of the audit, the budget had been revised to $18.6 million due to the reallocation of funds to the NAFIS upgrade and NCIDD in March 2003. However, CrimTrac has agreement from the BoM that it can draw from the remaining unspent NEPI surplus funds of $2.8 million to ‘top up’ the CPRS budget should this be required. At the beginning of 2003–04, some $13.8 million remained unspent from the CPRS notional allocation.\(^\text{14}\)

2.63 CrimTrac advised it faces several challenges in defining and delivering CPRS, given the differences in the operational systems of the police

\(^{13}\) ibid. p.31.

jurisdictions. There are also legislative difficulties and differences in interpretation of what constitutes a warrant, a minor crime, and a ‘spent’ conviction.\textsuperscript{15} In addition, a cultural change in police jurisdictions is required to fully adopt the nationwide sharing of information combined with the introduction of the technological platform proposed, whereby the systems will be hosted on a midrange system and accessed via a web interface and messaging system. CrimTrac had already expended some $3 million in early attempts to progress the programme.

\textbf{2.64} The jurisdictions visited during the preliminary study phase of the audit expressed some frustration at the lack of a completed deliverable for CPRS. This view was supported by other jurisdictions in their responses to the ANAO survey.

\textbf{2.65} CrimTrac advised that some of the early stumbling blocks were the need to make policy decisions about whether the system should be centralised or de-centralised, as well as whether it should contain only factual, known information or should have links to intelligence related data. There was less agreement among the jurisdictions regarding the end product required than was evident for the NAFIS and NCIDD systems.

\textit{The CPRS pilot project}

\textbf{2.66} At the time of the audit, CPRS was being progressed by a pilot project with two large jurisdictions, NSW and Victoria, known as the Minimum Nationwide Person Profile (MNPP).

\textbf{2.67} In recognition of the significant resources jurisdictions would be required to expend to assist in this pilot project, CrimTrac sought approval from the BoM in early 2003 to allocate some $100 000 each from the Australian Government funds to NSW and Victoria. The purpose of this allocation was to enable NSW and Victoria to determine the full costs of their participation. As at February 2004, the NSW estimate was about $1.6 million and the Victorian estimate was some $1.9 million.

\textbf{2.68} CrimTrac advised that the design stage of the pilot was progressing well, with jurisdictional agreement reached on the definition of some 26 data entities. CrimTrac was preparing for stage two of the pilot. The BoM had approved the allocation of $75 000 to each of the remaining jurisdictions for them to undertake the necessary planning and analysis to establish the full costs of their participation in the MNPP.\textsuperscript{16}

\textsuperscript{15} Convictions are deemed to be ‘spent’ once a specified amount of time has elapsed, and they are to be removed from a person’s criminal history records at this time.

\textsuperscript{16} This decision was made at the September 2003 meeting of the CrimTrac BoM.
2.69 The ANAO notes that the funding of work in the jurisdictions appears to be a departure from the original intention that the $50 million provided by the Australian Government would be used mainly for the development of systems by the CrimTrac agency, and that jurisdictions would be responsible for any costs incurred in adapting their systems to meet the CrimTrac systems. However, the IGA does not prevent the use of funds in this manner. The Australian Government Chairman of the BoM has a veto power over the expenditure of these monies.

**Conclusion on the status of the CPRS Capability Development Programme**

2.70 The ANAO concluded that, notwithstanding that CPRS was intended for delivery after the NAFIS and NCIDD, progress to date appears to be slow, and the costs not yet fully determined.

2.71 With respect to the MNPP pilot project, the ANAO concluded that this appeared to be a good approach to progressing this challenging programme.

2.72 The ANAO further concluded that, due to the implementation issues identified to date and the decision to fund work in the jurisdictions, there is a risk that CPRS will not remain within the notionally allocated development budget of $18.6 million from the Australian Government monies.

2.73 The ANAO concluded that several factors had contributed to the slower progress of CPRS. Some of these factors are addressed in more detail in Chapters Three and Four.

**Controlled access to appropriate information by accredited third parties**

2.74 Under the IGA, one of CrimTrac’s Broad Objectives is ‘providing controlled access to appropriate information by duly accredited third parties’. This is a continuation of a NEPI function.

2.75 Under the now titled National Criminal History Record Checking Programme, (the NCHRC), CrimTrac provides approved agencies (currently only government agencies) with criminal history information under legislative provisions.

2.76 The contribution to the CrimTrac Outcome is described as follows: This Programme minimises the risk of accredited agencies employing a person who is not fit to hold a position of trust due to adverse criminal history.
In particular, the risk of abuse of the young, the vulnerable and the infirm is reduced. The use of police data for social justice outcomes is maximised.\textsuperscript{17}

2.77 CrimTrac has continued to sign MOU with accredited agencies; implemented the first part of an electronic system to streamline processing;\textsuperscript{18} and implemented a new charging policy for use of the system.

2.78 During 2002–03, 431,604 checks were undertaken, resulting in 83,171 referrals to the jurisdictions for criminal offence history.\textsuperscript{19} CrimTrac anticipates a significant rise in business of up to 1.2 million checks per annum. The service enables the provision of national police service certificates for employment, licensing and other purposes.

2.79 Under the arrangements applying prior to 1 October 2003, agencies could seek information from either CrimTrac direct or from their State jurisdiction (where this service was available). Any agency conducting more than 500 checks per annum was (and still is) able to go directly to CrimTrac and apply for accredited agency status. Individuals seeking their own records had to apply to the jurisdiction in which they were resident. In the States and Territory where the service was not available, individuals were able to apply to the AFP for a national criminal history record check.\textsuperscript{20}

2.80 Jurisdictions set their own charging rates and CrimTrac charged the requesting jurisdiction a small flat fee for each initial check on the NNI. CrimTrac then paid the relevant jurisdiction a higher fee if a match occurred and further investigation or criminal history information was required. CrimTrac charged the agency requesting the check a fee based on a sliding scale that was dependant on the monthly percentage of matches.

2.81 CrimTrac has been working, and continues to work, with the jurisdictions to determine how the increasing demand from the public and private sectors will be met.

2.82 After a pricing review conducted by Access Economics, CrimTrac set the central price, on a per check basis, for all record checking at $22.00 for commercial organisations, $18.50 for individuals and government organisations, and $5.00 for volunteers. Jurisdictions may impose an administrative handling fee above the central CrimTrac fee. The new pricing model came into effect for three States and a Territory from 1 October 2003.

\textsuperscript{17} op. cit. Second Annual Report 2002–03. p.35.

\textsuperscript{18} This is called the External Agency Management System (EAMS).

\textsuperscript{19} Performance Management Report Service Delivery to Accredited Agencies, CrimTrac 14 July 2003. Section 1.1.

\textsuperscript{20} Subsequent to October 2003, it became compulsory for individuals wanting their own criminal history record check to apply to the jurisdiction in which they are resident.
another State commenced in December 2003 and the remaining States and Territory are scheduled to come on line from 1 July 2004.

2.83 CrimTrac advised the ANAO that the revenue to be generated could be sufficient to wholly fund CrimTrac’s recurrent budget within two years. In this way, jurisdictions’ annual subscriptions, currently based on authorised policing strength, could be replaced.

2.84 In responses to the ANAO survey, although the jurisdictions indicated that they perceived the enhancements to the NCHRC to be of potential benefit, they were critical of the manner in which CrimTrac had consulted on, and managed, these changes. Almost all commented that CrimTrac had focused on the potential benefits to be delivered in enabling the agency to become increasing self-funded and, consequently, had not placed enough emphasis on the views and needs of the jurisdictions and the potential impact on their resources.

2.85 In its response to the ANAO survey, CrimTrac indicated that it considers the implementation of the enhancements to have been protracted by legislative difficulties and lack of initial jurisdictional support for the changes. The CEO also acknowledged there had been staffing difficulties early in the implementation under CrimTrac.

2.86 An examination of the major sources of revenue to support CrimTrac showed that during 2003–04 there was a significant rise in revenue from NCHRC, and a corresponding drop in the annual subscriptions required from the police jurisdictions (Refer Figure 2.2, page 45). The forecast for 2004–05 shows that this movement is expected to continue.

2.87 The ANAO notes that there may be legal and social difficulties associated with the continued expansion of the NCHRC, such as changes to the definition of ‘spent conviction’ in differing legislation. Hence, there may be a need for ongoing vigilance and further implementation of appropriate controls over the approaches and procedures to make sure they are consistent with the Privacy Principles, natural justice and other legislative requirements. The ANAO was advised that National Vetting Guidelines are being developed.

Conclusion on the status of the NCHRC

2.88 The ANAO concluded that CrimTrac continues to provide this business deliverable and has made enhancements to the systems involved.

2.89 The ANAO also concluded that CrimTrac’s plans to use the NCHRC as a major basis for the agency’s ongoing funding appear to be soundly based. However, it was not possible to assess the overall impact on police jurisdictions from the data available, as well as any consequences this, in turn, may have on the future direction of the NCHRC.
Conclusion on the overall status of the key deliverables

2.90 Although the IGA did not specify particular timeframes for delivery, the Australian Government expected that significant progress would be made during the first three years and that the majority of the funds allocated by the Commonwealth of Australia would be spent within this time.

2.91 Overall, the ANAO concluded that CrimTrac’s progress in implementing the key deliverables has been variable. One database is fully operational; one system is constructed but yet to be loaded with all jurisdictions’ data; and two other projects are at the pilot and design phase. CrimTrac has made significant efforts to initiate each of the key deliverables specified in the IGA, with resultant pressures on the resources of the agency.

Figure 2.1

Key deliverable progress

<table>
<thead>
<tr>
<th>Key deliverable</th>
<th>NAFIS</th>
<th>NCIDD</th>
<th>NCSOS / ANCOR</th>
<th>CPRS</th>
<th>NCHRC (This service is not a key deliverable but contributes to a broad objective of the IGA)</th>
<th>Current status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Progress indicator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>deployed</td>
<td>developed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>designed</td>
</tr>
</tbody>
</table>

Source: ANAO analysis

2.92 The ANAO acknowledges that CrimTrac has faced significant challenges in its role of developing and delivering IT solutions to service nine police jurisdictions with varying approaches and systems, and with each operating under the constraints of differing Australian Government, State and Territory legislation.

2.93 In addition to this, CrimTrac has continued to deliver and maintain the former NEPI mainframe systems, as well as bringing into place the accountability and reporting mechanisms required to fulfil its obligations as a new Australian Government executive agency.

2.94 Although not all of the deliverables have been completed, significant progress does appear to have been made. The successful delivery of the CrimTrac projects is a collective endeavour, involving all the partners under the IGA. A number of the issues encountered under the previous NEPI Agreement have been resolved, with CrimTrac and jurisdictions all in agreement that CrimTrac is an improvement on the previous arrangement.
Additional deliverables

2.95 CrimTrac has also participated in additional projects that were not specifically identified in the IGA, but which fall within the ambit of supporting nationwide policing initiatives through the provision of high-quality systems.

National Handgun Buyback Support System

2.96 In response to the Council of Australian Governments’ resolutions made following the 2002 Monash University shooting incident, the Australian Government approached CrimTrac seeking the agency’s support to develop a National Handgun Buyback Support System (NHBSS).

2.97 The Australian Government, via the AGD, provided an additional $2.7 million in funds to CrimTrac in the last quarter of 2002–03. The project came with short timeframes and a target operational date of 1 July 2003. During 2002–03, some $1.2 million of this funding was drawn down.

2.98 CrimTrac developed this project under the CPRS area, using web-based and midrange technology. Key features of the system were to include: the provision of an online entry system; a weapons identification system; data security; an audit capability; and a transaction and reporting capability.

2.99 The NHBSS was to be built in conjunction with Victoria Police and was to be ‘hosted’ at CrimTrac. The enhanced weapons identification system is based on that used by Victoria Police, in line with CrimTrac’s adoption of ‘best-of-breed’ approach.

2.100 The system became operational in July 2003, with the exception of NSW and SA, who started using the system in October 2003. The initiative has been extended until 30 June 2004, when all jurisdictions will have completed their buy-back, with decommissioning of the NHBSS proposed by the end of June 2005, allowing for a final audit of the system to be conducted.

The Disaster Victim Identification Tool

2.101 Following the Bali bombing in October 2002, the CrimTrac BoM supported the use of NAFIS for crime scene evidence collection and the use of the DNA database for victim identification. The system, known as the Disaster Victim Identification (DVI) Tool, was deployed to the AFP to assist in the identification of victims of the bombing by matching DNA from body parts with DNA volunteered by relatives.

2.102 The DVI was based on the programme for NCIDD with the assistance of software provided by Queensland’s John Tonge Forensic Centre. The CrimTrac programmer subsequently received an award for the design of the system. Some 43 persons were identified using the DVI Tool.
2.103 NAFIS was used to identify a further twelve victims and was also used in the crime scene investigation processes.

Conclusion on the status of the additional deliverables

2.104 The ANAO concluded that CrimTrac had successfully progressed these additional deliverables.

Australian Government funding

2.105 As noted earlier, the Australian Government provided a one-off allocation of $50 million for the implementation of CrimTrac. It was envisaged that the monies would be expensed during the first three years of operation. However, CrimTrac sought an extension to this arrangement to draw down further monies during the fourth year of operation, 2003–04. CrimTrac’s actual and forecast revenues are shown in Figure 2.2.

Figure 2.2

CrimTrac actual revenue 2000–01 to 2002–03 and forecast revenue 2003–04 to 2004–05

Source: ANAO analysis of CrimTrac data

2.106 Figure 2.2 shows that CrimTrac will continue to expend the Australian Government’s $50 million in 2003–04 and 2004–05. It also shows the planned shift from jurisdictional subscriptions to increased fee revenue from the NCHRC in the forecast years.

2.107 The ANAO concluded that CrimTrac is likely to continue to use Australian Government monies for the immediate future since the agency will not be fully self-funded until July 2005, at the earliest. The ANAO noted that
expenditure of the Australian Government’s $50 million will take some six years, which is twice as long as originally planned.

2.108 At the time of the audit, some $17.1 million of the Australian Government funds remained unspent. These were notionally allocated to the CPRS, including the development of the NCSOS. CrimTrac had obtained approval from the AGD to continue to draw monies after the initial three-year period.

2.109 The rate of expenditure of the Australian Government monies by project is indicated below.

**Figure 2.3**


![Bar chart showing expenditure by year and project](https://example.com/bar-chart.png)

Source: ANAO analysis of CrimTrac data.

**Conclusion**

2.110 The ANAO concluded that CrimTrac has allocated the monies in accordance with the Australian Government’s intentions, but the rate of progress of the key deliverables and, hence, expenditure, has been slower than was originally planned. The consequences of this do not appear to be unduly disadvantageous, given the broad intention for ‘significant progress’ within the first three years. Subscriptions from the jurisdictions and revenue raised from the NCHRC and other sources fund the recurrent budget for the administration of the agency.
3. **Achievement of the Broader Objectives of the IGA**

This chapter discusses the progress CrimTrac has made in achieving the broader objectives of the IGA, as well as its ability to influence system delivery times through the timely resolution of key issues.

**Establishment of CrimTrac as a separate agency under the terms of the IGA**

3.1 CrimTrac advised the ANAO that its establishment by the Australian Government as an executive agency, under the AGD portfolio, was considered to have a number of advantages over the previous NEPI Agreement, including:

- transparency of funds management;
- the depreciation of the agency’s IT assets to fund replacement; and
- increased accountability and better reporting, in line with Australian Government standards.

3.2 The ANAO did not examine the issues of funds management, asset depreciation, and reporting in any detail during the performance audit. The ANAO conducts financial statements audits of CrimTrac annually. No major findings have emerged in relation to the management of funds and assets.

3.3 On 1 July 2002 CrimTrac also became a prescribed agency under the *Financial Management and Accountability Act 1997*, still under the auspices of the Attorney-General’s portfolio.

3.4 CrimTrac staff are largely employed under the *Commonwealth Public Service Act, 1999*. The agency brings in policing expertise through secondments from the jurisdictions, and also uses specialist assistance through IT contractors to progress the projects.

3.5 During 2002–03, there were 36 ongoing staff employed at CrimTrac plus 3 non-ongoing staff. CrimTrac supplemented these with some 20 contractors and 4 jurisdictional secondees. The total employee expenses to CrimTrac for 2002–03 was some $3.4 million.

3.6 The ANAO found that CrimTrac had made considerable efforts to deliver the range of formal reports and plans required under the *Financial Management and Accountability Act 1997*, in line with Australian Government standards.

---


22 ibid. p.90.
standards of accountability and reporting. CrimTrac advised the ANAO that it has a policy of reviewing these plans every two years. The Strategic Plan for 2004–2007 was being progressed at the time of the audit.

3.7 The ANAO considers that, in addition to progressing the key deliverables set out in the IGA and maintaining the former NEPI mainframe systems, CrimTrac has made considerable efforts to put in place the policies, procedures and reporting structures required of an Australian Government agency. In doing so, many of the issues relating to the former NEPI agreement appear to have been alleviated.

**Coordinated national policing information systems for a safer Australia**

3.8 CrimTrac’s Outcome is ‘Coordinated national policing information systems for a safer Australia’. Its Output 1.1 is ‘Facilitation of the delivery of high-quality national policing information services’.  

3.9 An examination of early documents relating to CrimTrac indicates that the underpinning intention was to establish a ‘national crime information system’ under a collaborative IGA, a partnership between the Commonwealth of Australia and each State and Territory in Australia. Recital A of the IGA states ‘CrimTrac is a major initiative being undertaken by the Commonwealth, State and Territory Governments’.

3.10 Such a partnership presents logistical challenges given the differences in priorities, policies, procedures, systems, resources and laws between each jurisdiction in Australia. In addition to these challenges, CrimTrac faced further obstacles to overcome the deficiencies and resultant tensions that were a legacy of the NEPI Agreement. The jurisdictions also needed time to adjust to having an Australian Government ‘host’ under the new IGA.

3.11 In order for such a complex and high-level partnership as that set out in the IGA to work in practice, the ANAO considers that the following factors need to be present:

- *a shared understanding of the objectives* of the agreement and how each project contributes to these and to the agency Outcome;
- *clearly defined and well understood roles and responsibilities* for each of the partners at both the strategic and the operational levels;
- *a clearly defined and understood consultative framework* that provides for all parties’ views to be represented; and

---

23 ibid. p.12.
Achievement of the Broader Objectives of the IGA

• a reporting framework that allows for the impact of the work achieved under the partnership agreement to be measured and/or assessed.

3.12 The ANAO examined each of these factors to assess the extent to which they were present, and to determine whether there were any weaknesses in the partnership approach that may be impeding the achievement of the broader objectives under the IGA and the CrimTrac Outcome.

A shared understanding of the IGA objectives

3.13 As specified in Clause 3.1 of the IGA, The broad objectives of CrimTrac are to enhance Australian policing through:

(a) the provision of high quality information services that:
   (i) meet the needs of the Australian policing community; and
   (ii) establish best-practice service models in relation to the provision of information to support policing; and
   (iii) are project-oriented and cost benefit driven to achieve outcomes.

(b) support for the jurisdictions in the implementation and use of CrimTrac services; and

(c) providing controlled access to appropriate information by duly accredited third parties.

3.14 Accordingly, CrimTrac’s role since inception has been one of developing, delivering and supporting systems that meet the needs of police, either through the key deliverables of the IGA or one-off additional deliverables.

3.15 The ANAO analysis suggested that links have not been well established between the objectives of the IGA, which is services that meet the needs of Australian police, and the CrimTrac Outcome of ‘Coordinated national policing information systems’.

3.16 By way of example, the CPRS includes a complex suite of projects that will coordinate, integrate and enhance a range of existing systems. As shown in Chapter Two, progress for the CPRS has been significantly slower than for the other key deliverables. CrimTrac advised that, although it is understood that the new products will enhance police safety and improve information flows, there is less clarity of vision about how the projects will operate as ‘Coordinated national policing information systems’. The ANAO considers that the CPRS projects have been, at least in part, hampered by a lack of a ‘shared’ vision.

3.17 This lack of a shared vision has resulted in debates over whether the systems should contain links to intelligence data, whether the systems should
be centralised or de-centralised, as well as over the specific data entities to be included and the resultant reports required.

3.18 The operational focus on the IGA broad objective of ‘…services that meet the needs of the Australian policing community’ has not served this project well. Although it is clear that all parties are focused on the progressive delivery of a range of systems to enhance policing, the ANAO considers that better definition of the links to the vision in the CrimTrac Outcome of ‘Coordinated national policing information systems’ may have assisted in better determining priorities, and providing a tighter focus on the end requirements.

Conclusion regarding shared understanding of the objectives

3.19 The ANAO concluded there would be benefit in CrimTrac seeking to better define the links between the objectives of the IGA and the CrimTrac Outcome. To do so would provide an increased understanding of the context of the CrimTrac projects, and a common goal for all parties to work towards.

Clearly defined and well understood roles and responsibilities

3.20 Well defined, and understood, roles and responsibilities for each of the CrimTrac partners is important at both the strategic and operational levels for the efficient progress of projects under the CrimTrac initiative.

3.21 The role of the APMC, the SOG, the CrimTrac BoM, the CEO and the ‘CrimTrac agency’ are set out in the IGA, and are expanded upon in the CrimTrac Charter of Governance.

3.22 The Charter of Governance provides additional definition of the roles of the individual BoM members, the Chairperson, the CEO, the CrimTrac executive group, the BoM secretariat and the Finances Committee.

3.23 However, the ANAO found little evidence that the roles of the jurisdictions and their relationship with CrimTrac had been addressed with the same rigour.

3.24 By way of example, under Clause 3.2 of the IGA, titled ‘Jurisdictions to cooperate’, it states ‘The parties agree to cooperate fully with each other to develop and deliver the objectives of CrimTrac through the entities and processes set out in this Agreement…’ There was no further clarification of what ‘cooperate fully’ actually means, other than to agree to provide funds for projects participated in.

3.25 In practice, the existing mechanisms for interaction between the jurisdictions and the agency are the APMC, the SOG, the BoM, the various project User Advisory Groups (UAG) and, in some jurisdictions, a CrimTrac liaison officer.
3.26 With respect to the role of CrimTrac, as perceived by jurisdictions, the ANAO was advised that initially the agency was perceived to be stepping beyond the IGA charter by trying to anticipate and suggest data entities and system designs that might be of use to jurisdictions. CrimTrac advised that jurisdictions were swift to assert that the systems were to be driven in accordance with jurisdictional requirements.

3.27 Jurisdictions, in their responses to the ANAO survey questions about whether they considered the role of CrimTrac had been, and continued to be, appropriate, made the following observations about its role:

Acceptable as long as the agency did not expand to include the handling of intelligence data.

It took some time to adjust to the Commonwealth playing a role, but yes, the role is appropriate if it continues to develop and maintain systems.

Yes, it is appropriate and necessary to improve interchanges of data at the national level, must be driven by jurisdictional needs.

Yes, if it is an IT bureau providing second-level computer support.

Yes, it is an information management and distribution agency based around systems to meet police needs.

The focus should be to fulfil its primary role as a facilitator of information services for and to its clients.

Philosophically no, the role and governance models should have been better defined.

3.28 It is clear from these responses that jurisdictions mainly perceive the role of CrimTrac to be that of developing systems to meet their needs. For this to be achieved effectively, jurisdictions need to ‘drive’ CrimTrac by setting priorities for the delivery of specified systems and by ‘driving’ the content of these systems.

3.29 At the highest level, the APMC considers the strategic directions for CrimTrac and approves the agency’s Strategic Plan, as well as any new initiatives that require legislative or funding consideration. At the next level, the role of the BoM is to make decisions on behalf of the CrimTrac agency and also to represent the views of the jurisdictions.

3.30 As BoM members, the Commissioners approve decisions regarding the commitment of CrimTrac funds to various projects or administrative functions. They also agree to the level of subscriptions or depreciation levies to be supplied by the jurisdictions. In this way, the jurisdictions ‘cooperate fully’ as per the IGA.

3.31 However, in this collective capacity as BoM members, the Police Commissioners do not appear to make decisions regarding the commitment of
the respective jurisdictional resources necessary to make any systems or procedural changes in the jurisdictions. Often, jurisdictional changes are required for the CrimTrac projects to be fully delivered. The jurisdictional support is then decided on an individual basis once each project commences.

3.32 The ANAO found no evidence of any discussion or agreements about whether ‘cooperate fully’ included the subsequent allocation of priority or resources to progress CrimTrac initiatives outside of the central agency itself. The ANAO noted several papers and reviews relating to communication issues, and the need to set cooperative strategic directions. However, none of these addressed the underlying responsibilities of the jurisdictions as signatories to the IGA.

3.33 The consequences of this appear to be two-fold. First, there is some lack of clarity regarding who is to ‘drive’ the various projects and the resultant elements of work to be undertaken. Second, the potential exists for a mismatch in the allocation of priority to CrimTrac development work (in the central agency) compared to the priority attached to work in the participating jurisdictions.

3.34 One of the jurisdictions, in its response to the ANAO survey, expressed frustration that CrimTrac had been slower than anticipated to deliver the CPRS, but also stated that jurisdictions had abrogated their responsibility to provide clear directions to the agency.

3.35 The ANAO considers that the CrimTrac initiative has been established with the intention of it being a team with nine partners—the Commonwealth of Australia (as represented by a Commonwealth member of the BoM and the AFP as a jurisdiction) and the eight State and Territory police jurisdictions. The initiative is likely to work most effectively where the roles and responsibilities of all nine team partners are clearly defined and understood by all.

3.36 The ANAO considers that, in order to strengthen the partnership approach, CrimTrac would benefit from the establishment of a clear definition of, ‘jurisdictions to cooperate fully’ that better aligns the priorities of CrimTrac and jurisdictional work. This should be supported by a mechanism for the allocation of jurisdictional priority, and resources, to progress work in the jurisdictions that corresponds with the priority being allocated to central CrimTrac work.

3.37 The ANAO notes that, although this could be achieved in part by clarifying the arrangements to apply during the scoping for each project, there are advantages in seeking a high-level agreement; that is, where clear definitions are agreed and understood by all partners regarding their respective roles and responsibilities, in order to facilitate the efficient progress of CrimTrac projects.
Conclusion regarding clarity of roles and responsibilities

3.38 The ANAO concluded that the IGA has limitations with respect to the partnership approach. We further concluded that CrimTrac should establish a formal agreement, such as an MOU, between all the partners as the basis for clearly defining the expected responsibilities of each partner in their role as a signatory to the IGA. This would assist the partnership approach under the IGA to be maximised.

Recommendation No.1

3.39 The ANAO recommends that, to supplement the Inter-Governmental Agreement, CrimTrac seek to establish a formal agreement between all the partners that clearly defines the agreed roles and responsibilities of each partner.

CrimTrac response

3.40 Agree. CrimTrac would prefer to have a set of guiding principles, as MOUs can be cumbersome and consensus has proven to be difficult and expensive to achieve. Jurisdictions may opt not to participate in all initiatives and are keen to preserve this right, as set out in the IGA.

A clearly defined and understood consultative framework

3.41 As stated in paragraph 3.11, the ANAO considers that, in a complex partnership, there needs to be a clearly defined and understood consultative framework for all parties’ views to be represented. The ANAO found that CrimTrac had recognised the need for a clearly defined framework and had applied a number of initiatives to address this requirement.

3.42 CrimTrac set out its key lines of reporting in its Charter of Governance. The agency also initiated reviews to examine options for improving its communication and consultative mechanisms with the jurisdictions. In 2002, CrimTrac commissioned Wilton Hanford Hanover, a consultancy firm, to review the agency’s communication strategies. The consultant’s report was delivered in July 2002.

3.43 The key findings from this report were the need for:

- immediate refreshing of the strategic case for CrimTrac, commencing with the development of a substantive rationale statement, developed collaboratively;

- commencement of processes to develop synergy with jurisdictional strategic and operational planning, including development of joint business cases and transparent pricing policies; and
• development of a corporate information programme underpinning strategic agency goals that includes repositioning of the agency, issues management and proactive media capabilities.

3.44 The report highlighted a range of issues, including ongoing tensions relating to the former NEPI, that staff at CrimTrac felt they were struggling with in order to understand the value-add they contributed to jurisdictions, and that the project governance and reporting mechanisms were not working to support partnering arrangements.

3.45 The report put the onus on CrimTrac to develop communication strategies and appropriate administrative policies. The ANAO notes that the report, although making references to partnering, did not address the corresponding strategies that might be required from the jurisdictions to support partnering.

3.46 The ANAO found that CrimTrac had developed a Communications Policy that addressed the more procedural aspects of providing briefings and meeting the Australian Government guidelines for correspondence and answering parliamentary questions. Section 1.5 of the Communications Policy states:

The Communications Policy is not to be confused with the Communications Strategy that will identify key communications issues and messages relevant to CrimTrac. The Communications Strategy will also provide a framework that will enable CrimTrac to facilitate effective cooperation with its stakeholders.

3.47 The ANAO was advised that the Communications Strategy is still being developed.

3.48 The ANAO also reviewed a draft document titled ‘CrimTrac Projects—Jurisdictional Engagement Guidelines’. Although intended for in-house use only, the status of this document was unclear. Nonetheless, the ANAO noted that it also focused on the protocols for CrimTrac to communicate with jurisdictions, but did not address the return protocols.

3.49 CrimTrac continues to try to address the issue of communication and effective consultation, and continues to explore mechanisms that would better align CrimTrac with the jurisdictions’ strategic and operational directions. In 2003, a Policing Information Exchange Strategy was prepared.

3.50 The strategy has evolved with the Police Commissioners Policy Advisory Group (PCPAG) paper titled: ‘Jurisdictional Requirements for the Strategic Direction of CrimTrac’. This document identifies ‘gaps in both high level strategic direction for policing as it impacts upon CrimTrac and in the way police and CrimTrac deal with each other on existing projects’. 24

3.51 The PCPAG recommended that the CrimTrac BoM establish a Strategic Issues Group (SIG) to provide ongoing strategic policy advice and to facilitate the resolution of legal, policy and other issues that arise between police jurisdictions and CrimTrac. The SIG is also to look at ways to better identify CrimTrac project parameters as well as identifying and reporting the cost components of each stakeholder.

Conclusion regarding a clearly defined and well-understood consultative framework

3.52 The ANAO concluded that the PCPAG initiative will improve the strategic consultation and communication framework between CrimTrac and the jurisdictions, and should assist CrimTrac to better align its projects to continue to meet the current and future needs of police.

3.53 However, the ANAO further concluded that the PCPAG initiatives should be underpinned by a strengthening of the shared vision and greater clarification of the roles and responsibilities of the IGA signatories. The new strategies will work best in an environment where the partnership vision and the roles and responsibilities of all signatories to the IGA are transparent.

A reporting framework that measures agency impact

3.54 Holistic reporting of an agency’s achievements at the Outcome level can assist in fostering and sustaining a shared understanding of the overall objectives and impact of an agency’s work.

3.55 The ANAO notes that CrimTrac’s Outcome of ‘Coordinated national policing information systems for a safer Australia’ is difficult to measure and, hence, to report against.

3.56 Each of the key deliverables, such as NAFIS and NCIDD, has its own performance measures, including a statement regarding its ‘contribution to the CrimTrac Outcome’. For example, the NAFIS contribution is described as: ‘NAFIS assists police in establishing identity from fingerprints and palm impressions more quickly and reliably and contributes to the solving of crime’.

3.57 However, it is not possible to report effectively against the NAFIS Outcome without all jurisdictions collecting comparable data, for example, regarding the number of cases NAFIS was used in, and the time taken to resolve these cases. The only information available regarding NAFIS’ contribution to policing is at a theoretical level. The CrimTrac Annual Report for 2002–03 states that: ‘The matching results achieved against the palm database have significantly improved the ability of police to resolve volume

and major crimes across Australia’. The report did not cite any supporting data.

3.58 Consequently, the NAFIS performance measures focus on CrimTrac controlled aspects, including the quality, quantity and price of the system. Operational aspects, such as the availability of the system, define these elements.

3.59 The ANAO acknowledges that it is difficult to measure the actual impact of the agency on ‘Coordinated national policing information systems’. However, it may be useful to develop some measures that show what is collectively being achieved. CrimTrac advised that the SIG will be tasked with defining best practice and performance analysis processes for NAFIS by December 2004.

**Conclusion regarding a reporting framework that measures agency impact**

3.60 The ANAO concluded that there are difficulties in effectively measuring, and hence reporting, against CrimTrac’s Outcome. However, the ANAO further concluded that there might be benefit in CrimTrac, in consultation with its partners, considering ways of better measuring and/or assessing what is collectively being achieved.

**Framework for timely resolution of key issues**

3.61 Given the complexity of some of the systems to be delivered, and the number of stakeholders potentially involved, the ANAO considered whether CrimTrac had in place a framework for key problematic issues to be addressed and resolved in a timely manner.

3.62 CrimTrac is primarily accountable for the timely development of its systems in an environment where it largely has no apparent influence over some of the fundamental aspects required to achieve its responsibilities. Given this, it is important that CrimTrac has access to a framework that enables it to draw the attention of the key stakeholders in its environment to issues/problems that are impacting significantly upon the agency’s ability to deliver its systems, and hence, to fulfil its objectives under the IGA.

3.63 Under its project management methodology, CrimTrac programme and project managers may escalate issues to the CEO as necessary. In this way, CrimTrac had implemented a framework for the internal resolution of issues.

---

26 ibid. p.15.

27 Although the NAFIS performance measures focus on factors under CrimTrac’s control, the jurisdictions agree to the performance standard and measures to be applied.
3.64 During the audit, the ANAO was advised that CrimTrac had established ‘project champions’ to progress issues relating to particular projects, such as a delay in responses from some jurisdictions that may adversely influence overall project progress. CrimTrac also established the SIG as a mechanism for more quickly identifying strategic issues that may become problematic. The ANAO considers these to be sound initiatives.

3.65 However, it was unclear to the ANAO how key issues beyond the capacity of internal resolution by the agency and its partners, such as amendments to legislation, were to be managed or progressed. The ANAO found no evidence of a framework containing procedures, or guidance, indicating when and how issues should be drawn to the attention of external stakeholders.

3.66 As an example, the operational ‘deployment’ of NCIDD has been delayed by almost three years pending the resolution of legislative amendments to allow for cross-jurisdictional matching to occur. Once the legislation has been amended in each State or Territory, a specific MOU in relation to the NCIDD must be signed between CrimTrac and each State and Territory, as well as a Ministerial Arrangement between each State and Territory to agree to the matching conditions.

3.67 ANAO examination of the BoM minutes showed that the legislative issues became apparent in mid 2001, once the central database and matching engine were complete and jurisdictions were invited to upload DNA profiles.

3.68 The Commonwealth of Australia legislative amendments are monitored by AGD as the agency responsible for legislative reform. CrimTrac also tried to monitor the progress of the legislative reform, as well as to overcome some of the practical issues, through participation in three workshops.

3.69 The ANAO notes that CrimTrac tried to progress the issue in late 2001. At the BoM meeting of November 2001 it was agreed that the Chairman would ‘report to APMC on the inhibiting effect of legislative complexities affecting NCIDD’. Subsequently, at the APMC meeting of July 2002, the APMC passed a resolution to ‘expedite agreements between jurisdictions to facilitate the exchange of DNA information in accordance with each jurisdictions’ legislation to dissolve disparities’.

3.70 The impact of the agency’s efforts and the APMC resolution is unclear to the ANAO, since the legislative amendments and the majority of MOU were still not finalised in March 2004. Legislative reform is not easily expedited, and in this case involves not only the Australian Government but also each State and Territory’s government.
3.71 The ANAO notes that delays in legislative amendments are clearly beyond the scope of the CrimTrac agency to resolve. However, given the importance of resolving these issues before NCIDD could be deployed, the ANAO considers it would have been beneficial for CrimTrac to have in place a framework for the timely progression of such a key issue, by drawing it to the attention of external stakeholders, and clearly articulating the consequences of ongoing delays as a prompt for action by the stakeholders to assist CrimTrac to alleviate the blockages.

3.72 The ANAO further notes that other CrimTrac systems, such as NCHRC, ANCOR and CPRS, also require the alignment or mutual recognition of Australian Government and State and Territory legislation before data can be matched across jurisdictions. In the absence of an adequate framework for the timely progression of these issues, there is a risk that other CrimTrac projects will also be significantly impeded.

3.73 The ANAO notes that CrimTrac’s link to the AGD is through the Chairman of the BoM and that the agency provides briefings to the department, the Minister for Justice and Customs, or the Australian Government Attorney-General when requested to do so. The ANAO considers there is a distinction between providing briefings and having in place a framework to elicit support for action.

3.74 The Minister or the Attorney-General may be able to bring priority to the legislative reform through the State Council of Attorneys-General, or by drawing the issue to the attention of the Prime Minister. This action could be appropriate given that the deployment of an important system such as NCIDD, and its contribution towards the Outcome of ‘Coordinated national policing information systems’, is presently being significantly impeded.

3.75 The ANAO considers that CrimTrac would benefit from the development of a framework and procedures for the timely resolution of key issues. The ANAO also considers there would be benefit in CrimTrac focusing on its Outcome when drawing stakeholders’ attention to key issues.

Conclusion regarding the framework for the timely resolution of key issues

3.76 The ANAO acknowledges that CrimTrac is not solely responsible for the progression of relevant legislative reforms. However, the ANAO concluded that the absence of a framework for the timely resolution of such key issues results in the risk of delays to CrimTrac projects, and an accompanying less efficient use of the agency’s resources.

3.77 In summary, the deployment of the deliverables under the objectives of the IGA, and hence the achievement of the CrimTrac Outcome, are likely to continue to be subject to legislative amendment issues. The ANAO considers
that CrimTrac should consult with its key stakeholders to seek the means to develop a framework for the timely resolution of key issues, on the basis that they pose a risk to the CrimTrac Outcome as well as to the particular projects concerned.

**Recommendation No.2**

3.78 The ANAO recommends that CrimTrac consult with its key stakeholders to develop a framework for the timely resolution of key issues that pose a risk to the CrimTrac Outcome or to particular projects.

*CrimTrac response*

3.79 Agree. CrimTrac notes ANAO’s acknowledgement that delays in legislative amendments are clearly beyond the scope of the CrimTrac Agency to resolve but that CrimTrac had made effort to influence the progression of legislation issues affecting NCIDD. This included escalation to the APMC in accordance with the governance defined in the IGA. CrimTrac is of the view that by using this established governance all stakeholders have been made well aware of NCIDD legislation issues.

**Conclusion regarding achievement of the IGA broader objectives**

3.80 The ANAO concluded that the establishment of CrimTrac as an Australian Government agency has resulted in the alleviation of many of the issues of its predecessor, NEPI. Although progress in some projects has been slower than anticipated, CrimTrac has progressed the key deliverables; implemented many internal plans and controls; and has continued to provide support for the former PRS systems.

3.81 The ANAO concluded there would be benefit in CrimTrac seeking to better define the links between the broad objectives of the IGA and the CrimTrac Outcome of ‘Coordinated national policing information systems for a safer Australia’.

3.82 The PCPAG initiative will improve the strategic consultation and communication framework between CrimTrac and the jurisdictions and should assist CrimTrac to better align its projects to continue to meet the current and future needs of police. However, the new strategies will work best in an environment where the partnership vision and the roles and responsibilities of all signatories to the IGA are transparent.

3.83 The ANAO also considered that it is difficult for CrimTrac to measure and report against its stated Outcome. However, the ANAO further considered there would be benefit in CrimTrac, in consultation with its partners, seeking the means to better reflect what is collectively being
achieved, which would benefit both efficient and effective management and enhanced external accountability.

3.84 The deployment of the key deliverables is likely to continue to be subject to legislative amendment issues. The ANAO concluded that CrimTrac should consult with its major stakeholders to seek the means to develop a framework for the timely resolution of key issues, on the basis that they pose a risk to the CrimTrac Outcome as well as to the particular projects concerned.
4. Project Management

This chapter examines whether CrimTrac has planned and managed its projects to deliver them efficiently and effectively.

Introduction

4.1 CrimTrac’s main business focus is on the efficient and effective management of IT projects. As previously identified, CrimTrac’s deliverables include a diverse range of systems that encompass:

- a variety of functionalities, from fingerprints to national vehicles of interest;
- IT platforms that include mainframe, midrange and customised solutions;
- funding arrangements with the IGA partners that vary according to need; and
- flexibility of project approach as required by the circumstances (for example, MNPP as a pilot with two jurisdictions (building a completely new system), and NHBSS (leveraging from a best-of-breed IT solution).

Project funding

4.2 At the time of the audit, CrimTrac had in place three project funding models.

4.3 The first model was used to complete the NAFIS and NCIDD Projects, where Australian Government funds were expended solely on tasks completed at CrimTrac, and jurisdictions funded work completed in the particular jurisdiction.

4.4 The second was employed for the CPRS Minimum Nationwide Person Profile (MNPP) Pilot Project. Under this approach, the Australian Government funding was used not only for the project design and development tasks undertaken at CrimTrac, but also to fund the pilot tasks in the two participating jurisdictions. All other jurisdictions were also provided with an amount to enable them to estimate the cost of their full participation in the MNPP.

4.5 A further approach was being used for ANCOR, in accordance with the APMC resolution that the system was to be one-third funded from the Australian Government, and two-thirds funded by the jurisdictions.
Audit approach

4.6 The ANAO examined CrimTrac’s project management, and how effective this has been in assisting the agency to deliver its various projects efficiently and effectively. As noted earlier, it was envisaged that ‘significant’ progress would be made within the first three years of the agency’s operation. CrimTrac subsequently set internal milestones for the delivery of each project as it was developed.

4.7 The ANAO also examined whether CrimTrac had an agreed project management methodology, whether it is applied in practice, and whether it contains any weaknesses that may impede efficient and effective delivery of the agency’s projects. The ANAO further examined whether CrimTrac had provided appropriate skills development for its project management staff.

CrimTrac project management methodology

4.8 The ANAO examined whether CrimTrac had in place a formal project management framework and methodology that would set out organisational expectations; provide a rationale or justification for more detailed procedures; and facilitate a consistent approach to project management across the organisation.

4.9 CrimTrac advised the ANAO that initially it had based its project management practices on two methodologies: Rob Thomsett Project Management methodology and/or PRINCE2. However, the agency did not formally specify how this methodology was to be applied to the CrimTrac projects.

4.10 In late August 2002, CrimTrac introduced its ‘Corporate Programme and Project Management Framework’ (CPPMF). This was designed to provide the framework for CrimTrac to detail its internal project management procedures. It also articulates relationships with the Project Coordination Committee (PCC), which was established in January 2002, as well as with the CEO and the BoM.

4.11 The CPPMF was made available to staff on CrimTrac’s intranet. CrimTrac also established a project management office (PMO), staffed by one CrimTrac officer, whose role was to provide additional support to the programme/project managers.

4.12 The CPPMF covers project definition, project management structure and processes, roles and responsibilities, reporting processes, quality control, risk management, and reporting templates.

4.13 Under the CPPMF, the project management structure and paths of communication are outlined in Figure 4.1. These were mainly applied to CPRS
projects and NCSOS. The Project Board model was introduced for the MNPP Pilot Project in 2003.

**Figure 4.1**

*CrimTrac project management structure and paths of communication*

Source: ANAO analysis adapted from CrimTrac’s CPPMF.

**Conclusion regarding CrimTrac’s project management methodology**

4.14 The ANAO concluded that CrimTrac had an appropriate project management methodology in place in PRINCE2. CrimTrac had endeavoured to support this with an internal project management framework, the CPPMF.

---

28 NAFIS and NCIDD were designed and developed prior to the introduction of the CPPMF in August 2002.
Both of these were available to all staff, together with other project support mechanisms, such as the PMO.

CrimTrac Programme and Project Management Framework issues

4.15 The ANAO examined how well the project management methodology and framework had been implemented, and whether these were effectively assisting CrimTrac in the management of its projects. PRINCE2\(^{29}\) is a recognised project management methodology. The ANAO did not examine this aspect, but focused on the use of the CPPMF as the key tool by which CrimTrac projects are managed.

4.16 The ANAO found that the agency had implemented the intent of the CPPMF. The project reports were prepared using the reporting templates. The PCC met every two to three weeks between January 2002 and mid 2003, and then met monthly.

4.17 However, ANAO examination of the CPPMF, as well as the project documentation supplied to the PCC, the BoM and selected UAGs, found some weaknesses in the CPPMF methodology, the manner of its implementation and in the project governance structures. The ANAO considers that these weaknesses had an impact on CrimTrac’s ability to efficiently coordinate its projects.

4.18 The issues, which are addressed in further detail below, include:

- inconsistent application of the project definition;
- lack of policies and project management guidance for project managers in how to effectively apply the CPPMF;
- lack of clarity in the roles and responsibilities for the project partners;
- gaps in the PCC’s role as coordinator of projects; and
- lack of timely provision of project management skills development for relevant staff.

Inconsistent application of the project definition

4.19 The ANAO considers that, in order for projects to be managed effectively, there needs to be clear definition and understanding of what constitutes a project and consistent identification of tasks as projects.

---

\(^{29}\) The PRINCE project management methodology was established in 1989 by the Central Computer and Telecommunications Agency in the United Kingdom. It was developed to manage IT based projects and was replaced in 1996 by PRINCE2.
4.20 CrimTrac has regarded the ‘development’ phase of the key deliverables to be projects. Once they are ‘deployed’, the systems become ongoing business deliverables or programmes, and the funding basis shifts from use of the Australian Government monies to the agency’s recurrent budget. The ANAO notes that systems undergo periodic upgrades or further enhancements, such as the connection of Livescan devices to NAFIS.

4.21 In addition to the key deliverables under the IGA, CrimTrac has an underpinning suite of ‘common services’ and infrastructure projects, for example, the rationalisation of the network.

4.22 The CPPMF states that CrimTrac is to define what constitutes a project using the PRINCE2 definition of ‘a management environment that is created for the purpose of delivering one or more business products according to a specified business case’.

4.23 Notwithstanding this definition, the ANAO found that the project definition was inconsistently applied, and that not all work carried out by CrimTrac was considered a project. For example, NCIDD was initially managed as a project. Once CrimTrac considered the database to be ‘developed’, it was considered to have been ‘delivered’, and hence was no longer deemed to be a project. As such, it was not subject to the CPPMF governance and reporting framework. As stated previously, the NCIDD Project had not been fully ‘deployed’ due to the legislative amendments required. At the time of the audit, only two States had data loaded into the system. The ANAO further found that the data security component of the NCIDD was not fully developed (see Chapter Five).

4.24 Although reports on the overall progress of the design and development of NCIDD were provided to the BoM, the ANAO found few reports to the PCC on NCIDD legislation or data security issues. The project scope did not appear to include the management of the deployment of the system. The ANAO notes that the CPPMF states that ‘all work that CrimTrac proceeds with should be treated as a project, this includes contractors’.

4.25 The ANAO considers that, if the PCC is to play an effective role in the coordination of projects and the monitoring of resources, it is important that all projects are identified as projects, and remain identified as such until deployment is complete. The CPPMF methodology should be applied consistently across the project continuum.

Conclusion regarding the application of the project definition

4.26 The ANAO concluded that CrimTrac should ensure that all future projects are identified formally as being projects, and remain identified as
such, until deployment is complete, and accordingly are brought within the CPPMF for monitoring and reporting. In this way, all projects will be subject to a consistent approach, and the agency’s resources and progress can be better allocated, monitored, and reviewed.

Lack of policies and project management guidance

4.27 It is important that clear guidance is provided to avoid the different interpretation and application of project management procedures, resulting in inconsistent project management. Such inconsistency also reduces the quality of information recorded that is to be submitted to senior management for the coordination of resources.

4.28 Clear guidance assists managers in determining the appropriate project management approaches for tasks, and provides assurance to CrimTrac that minimum standards are being met. The ANAO found that the CrimTrac programme and project managers were selected from a diverse range of backgrounds, including Australian Government programme managers from other agencies, seconded police officers, forensic scientists and/or IT experts.

4.29 After an examination of the CPPMF documentation, the ANAO considered that although the CPPMF provides reporting templates, it does not provide sufficient policies and guidance for project staff on how to complete the required project documentation.

4.30 By way of examples, the CPPMF does not include any policy or guidance on what cost estimates are to be included as part of project budgeting, nor on how to calculate the benefits to be realised from the project. The risks of not providing adequate policy and procedural guidance on these critical issues are outlined below.

Costs estimation

4.31 Every project should have a budget that identifies the costs over its whole life. It is also important to identify any second-order costs borne by other parties, both within and outside the agency, or its impact on other projects.

4.32 However, CrimTrac’s guidance under the CPPMF was limited to stating in the various project reporting templates under the heading ‘budget’, that programme managers are to provide ‘a detailed breakdown of the expenditure expected for the project, include everything [sic]’.

4.33 The ANAO found that, as a consequence of CrimTrac not having a formal policy and guidance on what was to be included in project cost

\[31\] ibid. p.34.
estimates and how this was to be calculated, project cost estimation across the agency was variable. In one instance, the ANAO found that a project had been approved without a budget.

4.34 In the absence of consistent and comprehensive cost estimation in the project start-up phase, there is a risk that project budgets will continually increase as the project progresses and further costs are identified.

4.35 The ANAO found several examples of project budgets being revised. For example, the Australian Government’s notional allocation for Phase I of the MNPP was some $4.1 million. At the September 2003 BoM meeting, this was revised to $6.8 million, an increase of 66 per cent. The completion date for MNPP Phase I was revised from January 2004 to end August 2004, leaving a potential risk for further cost revisions.

4.36 Some jurisdictions, in their survey responses, indicated that CrimTrac needed to improve its ability to scope projects and to better estimate the costs to the agency and to the participating jurisdictions. Nearly all jurisdictions were critical of CrimTrac for not undertaking a more comprehensive cost-benefit analysis of the NCHRC new funding model. Although a review was commissioned as part of the policy development, jurisdictions considered that it did not adequately examine the impact on them.

Benefits realisation

4.37 The ANAO found that, in a similar manner, there was little guidance on what programme managers should include to describe how the realisation of the project benefits would be assessed and measured in contributing to CrimTrac’s Outcome.

4.38 CrimTrac programme managers provide the BoM with project briefs and plans for approval. However, the ANAO found that the project plans did not provide a comprehensive analysis of the project benefits.

4.39 The ANAO concluded that, in order to assist CrimTrac and the participating jurisdictions to make decisions on whether projects should be conducted or not, consideration of the full costs and full benefits of the project should be undertaken. This would: assist CrimTrac to better service jurisdictions; enable the agency to report more fully to the BoM and the APMC on the relative merits and costs of each project; and, hence, assist in the better allocation of resources across competing demands. As discussed earlier, there is scope for CrimTrac to better report against its Outcome. It will be difficult for CrimTrac to do this without determining the full costs and benefits of each project.

4.40 The ANAO noted that CrimTrac was examining options for obtaining more comprehensive costs and benefits information for its projects and that the issue had been raised in the PCPAG paper.
Conclusion regarding the lack of policies and project management guidance

4.41 The ANAO concluded that there are risks to CrimTrac in not providing adequate policies and guidance on its project management procedures. The agency and its partners under the IGA would benefit from the development of policies and more detailed guidance, as the basis for a more consistent and comprehensive approach to the management of its projects.

4.42 In particular, the ANAO further concluded that CrimTrac should determine the full costs and benefits from its projects, in order to improve the cost estimation and scoping of these projects as well as to provide better information to assist in the strategic selection of new projects.

Recommendation No.3

4.43 The ANAO recommends that CrimTrac strengthen its project management approach through enhancing its CrimTrac Programme and Project Management Framework by:

(a) providing supporting policies and more detailed procedural guidance to programme and project managers; and

(b) measuring and/or assessing the full costs and benefits of its projects.

CrimTrac response

4.44 Agree. CrimTrac recognises that effective project management is essential to its success and has taken a number of steps to improve its project management environment since 2000:

- It employs professional project managers;
- It has required all staff to attend the PRINCE2 foundation project management course (a 4-day intensive course conducted by fully accredited PRINCE2 training provider);
- PRINCE Plus is available online to all staff, enabling them to use all the templates with online help and system navigation;
- It employs an accredited PRINCE2 full-time Project Management Officer to provide expert advice to any agency personnel in the use of the methodology and to provide an independent source of scrutiny for particular projects;
- It has commissioned an external review of its project management to assess the areas in which this may be improved. Following the Board’s endorsement of recommendations of that review in February 2004, the Agency has acted to inculcate better project management and governance across all active projects.
Lack of clarity in the roles and responsibilities for the project partners

4.45 Many government programmes and projects require coordination and cooperation between agencies, and parts of agencies, to achieve their goals efficiently. Experience has shown that such ‘joint delivery and management’ can pose management challenges as organisational priorities and processes may not always coincide. This is particularly the case when arrangements involve different levels of government, such as State/Territory and Australian Government delivered programmes, where several sets of differing priorities, procedures and standards apply.

4.46 As stated earlier, clearly defined roles and responsibilities at both the strategic and operational levels are required (Chapter Three). The ANAO examined the various roles and responsibilities assigned to those involved in the development and delivery of CrimTrac’s projects, and also examined the CPPMF to ascertain how well these were defined for CrimTrac programme and project managers.

Operational roles and responsibilities

4.47 Broadly, under the CrimTrac initiative the CrimTrac agency is the overall ‘project manager’ that initiates, coordinates and manages the various project processes. On the other hand, the jurisdictions are the ‘drivers’ of the nature, content and user requirements of the systems. The jurisdictions are also the ‘project managers’ for the changes requiring work in their respective jurisdictions.

4.48 At present, the roles of, and the relationships between, the CrimTrac ‘project manager’ and the jurisdiction ‘project managers’ are not well established, yet each project requires these to be in place for effective coordination.

4.49 The ANAO found that projects were sometimes delayed due to the need to make more complex decisions, the varying availability of resources and differing priorities being allocated to CrimTrac work. A number of jurisdictions described CrimTrac duties as being ‘over and above the daily duties’.

4.50 The ANAO noted that the project UAGs did not appear to have the authority to address project resource issues, nor to make policy decisions. Additionally, the ANAO found little evidence in CrimTrac’s documents that evaluated, or reported on, the progression of CrimTrac related work in the jurisdictions.

4.51 An examination of the CPRS UAG meeting minutes for 2002 and 2003, showed that jurisdiction resources were engaged in addressing other policing priorities. In the case of these projects, progress in responding to CPRS
requests appears to have been slow, but this was not reported directly and no revised milestone deadlines seem to have been set.

4.52 The ANAO found a lack of clarity regarding the mechanisms by which priority and resources could be assigned to the CrimTrac tasks in the jurisdictions at the project level. The ANAO considers that it must be difficult to progress projects in an efficient and effective manner if it is unclear how priority can be assigned to the projects, and adequate resources assigned accordingly.

4.53 The ANAO considered that the partnership arrangement for the CrimTrac initiative would be strengthened if the ‘process driver’ project managers in the CrimTrac agency have the means to better coordinate their work with their respective ‘project manager’ partners in the jurisdictions.

4.54 In a multiple agency environment, some agencies have addressed this via formal agreements, such as a Memorandum of Understanding (MOU) or a Business Partnership Agreement. These agreements provide a framework for specifying roles and responsibilities, priorities, accountabilities, reporting arrangements and performance management between agencies. They are, therefore, an important aspect for the governance of projects and programmes delivered by multiple agencies or parties.

4.55 Given the complex operating environment within which CrimTrac must develop and deploy its projects, such an agreement would be useful for:

- mandated projects that have a tight timeframe (for example, ANCOR); and
- complex projects where it is more difficult to reach consensus (for example the CPRS suite of projects) to prevent project scope creep and subsequent project ‘drift’.

4.56 The ANAO notes that CrimTrac and the BoM have already identified the above matters as an issue and are examining ways to address it. Part of the role of the proposed Strategic Issues Group (SIG), under the PCPAG proposal, will be to identify and monitor the costs of projects to jurisdictions, and to provide a central point of reference for advice on strategic issues that impact across CrimTrac projects and jurisdictions.

4.57 The ANAO considers that although there is a valid role for the SIG, the group may not alleviate the requirement for a direct link between CrimTrac as overall ‘project manager’ and the ‘project managers’ in jurisdictions.

4.58 The ANAO also notes that CrimTrac had commissioned a consultant to undertake a review of its project management methodology as it was applied to a recent project, the MNPP.
Conclusion regarding the operational roles and responsibilities

4.59 The ANAO concluded that there is scope for CrimTrac to clarify the operational roles and responsibilities of those involved in the management of its projects, as well as to provide greater guidance on how these parties are to interact.

4.60 The ANAO also concluded that CrimTrac would benefit from the establishment of a more formal framework or agreement between the agency and the jurisdictions involved in its projects, one that clearly defines the roles and responsibilities of the agency and jurisdiction project managers, including any accountabilities for project delivery.

CPPMF guidance on roles and responsibilities

4.61 At the operational project level, the CrimTrac CPPMF defines the roles and responsibilities of the Project Board, the CEO, the PCC, the PMO, programme and project managers, and team leaders. It does not describe how each of these is intended to interact with officers in the jurisdictions.

4.62 Although the CPPMF is intended to be an internal document, the ANAO considers that better practice would be to identify and detail the roles and responsibilities of all the parties involved in progressing a project. As discussed earlier, jurisdictions are not only the users of the CrimTrac systems; they also provide funds and resources and are major partners in the projects.

4.63 The consultative mechanisms that CrimTrac has established include: UAGs for each project (the CrimTrac project manager plus a representative from each jurisdiction); an IT Managers Group; and a Finance Managers Group. Some jurisdictions had also established a CrimTrac liaison officer, or unit, to coordinate the information flow between CrimTrac and the respective jurisdiction.

4.64 Although there is reference to these groups in the CPPMF, it does not describe their respective roles and responsibilities, nor detail how CrimTrac programme/project managers are to interact with them.

Conclusion regarding CPPMF guidance

4.65 As well as there being scope for CrimTrac to better articulate the strategic roles and responsibilities of the IGA partners, the ANAO found there was also scope for CrimTrac to more clearly define and establish the operational roles and responsibilities relating to individual project management.

4.66 The ANAO concluded that, in a multi-agency project environment, the project management framework should detail the respective roles and responsibilities of all the parties involved, and should provide guidance on
how the parties are to interact with each other to deliver the projects in an efficient and effective manner.

**Recommendation No.4**

4.67 The ANAO recommends that CrimTrac more clearly define, and set out in its overall project management framework, the roles and responsibilities of both the agency and jurisdiction project managers, including how the parties are to interact in order to progress the projects efficiently and effectively.

*CrimTrac response*

4.68 Agree.

**Gaps in the PCC’s role as coordinator of projects**

4.69 The efficient delivery of such a wide range of projects and supporting services as those managed by CrimTrac requires a sound strategic project management capability. The key coordinating and review bodies for CrimTrac projects are the BoM and the PCC.

4.70 The BoM approves projects at the strategic level. At the operational level, CrimTrac advised that the PCC is intended to be the review and coordination point for all of its projects. According to the CPPMF:

> The committee represents in PRINCE2 terms the Senior Suppliers and must deliberate on projects with that specific focus in mind. It is there to ensure that proposals for design and developing the products are realistic in that they are likely to achieve the results required by the Users within the cost and time parameters for which the Programme Manager is accountable. The role represents the interests of those designing, developing, facilitating, procuring, implementing, operating and maintaining the project products.

The PCC approves all major plans and authorises any major deviation from agreed stage plans in consultation with, and on behalf of the CEO. It is the authority that signs off the completion of each stage as well as authorises the start of the next stage. It recommends that required resources are committed and arbitrates on any conflicts within the project or negotiates a solution to any problems between the project and external bodies. The PCC operates on a consensus basis, any issues in dispute will be referred to the CEO.\(^{32}\)

4.71 The CPPMF further lists a broad range of responsibilities for the PCC that includes the approval of all project plans and the authorisation of any major deviations. The PCC Chair approves the decisions taken by the PCC members, and refers them to the CEO for approval and action as required. The PCC members are the CrimTrac executive, including the CEO, and the

\(^{32}\) Ibid. pp.13–14.
programme managers. The PMO supports the PCC and is required to coordinate the reports prepared by programme managers for presentation to the PCC.

**Operation of the PCC**

4.72 The ANAO reviewed the implementation of the PCC to determine whether it was assisting CrimTrac to coordinate the agency’s projects. The CPPMF requires the PCC to meet fortnightly. The ANAO found that meetings were held on average every two and a half weeks between January 2002 and mid 2003, and from then on were held monthly.

4.73 The ANAO considers that attendance at PCC meetings by all members is important for effective strategic planning and management of individual CrimTrac projects. However, the ANAO found that CrimTrac had cancelled two consecutive PCC meetings due to the unavailability of members. Of more significance was that the average number of members not attending meetings was four, and only one meeting was attended by all members.

4.74 In addition, the ANAO observed the following:

- the minutes reflected discussion centering on individual projects or tasks and there was little evidence of a ‘coordinated’ view to timing or resources;
- the minutes were brief—making it difficult to track any PCC decisions or the rationale for these decisions;
- there was inconsistent evidence of PCC decisions being ‘signed off’ and referred to the CEO for action;
- papers relating to projects were not always presented when requested by the PCC; and
- there was inconsistent presentation of the project template reports required under the CPPMF.

4.75 The ANAO tracked the NCSOS Project through the PCC meetings to test for the robustness of the CPPMF and the effectiveness of the role of the PCC. Table 4.1 shows the outcome of this tracking.
## Table 4.1

**Tracking of NCSOS Project via the PCC meetings**

<table>
<thead>
<tr>
<th>Date</th>
<th>PCC activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>21–Jan–02</td>
<td>PCC meetings commence.</td>
</tr>
<tr>
<td></td>
<td>7 Feb, 26 Feb, 12 March, 26 March, 9 April, 22 April, 7 May and 28 May—no reference to NCSOS.</td>
</tr>
<tr>
<td>18–Jun–02</td>
<td><strong>Project Initiation Report.</strong> Draft vision to be ready by 28 June 02. Project start up ideally ready for 12 July 02. CPRS Capability Development Programme UAG presentation and then to the BoM planned for August.</td>
</tr>
<tr>
<td>27–Aug–02</td>
<td>Project brief being developed for submission to PCC and the CPRS Capability Development Programme UAG on 6 and 13 Sep 02 respectively. No project report attached.</td>
</tr>
<tr>
<td>24–Sep–02</td>
<td>No meeting occurred on 6 Sep 02. <strong>Project brief</strong> attached. Updated version needed to be produced. No PCC decision taken.</td>
</tr>
<tr>
<td>8–Oct–02</td>
<td>No action, but agreed the <strong>Project Plan</strong> to be presented on 22 Oct 02.</td>
</tr>
<tr>
<td>11–Nov–02</td>
<td>No meeting occurred on 22 Oct 02. <strong>Project Plan</strong> approved in principle with minor changes. Requested changes are not specified.</td>
</tr>
<tr>
<td>17–Dec–02</td>
<td><strong>Project Plan completed and approved.</strong> No comment whether changes were taken up or if further changes were needed.</td>
</tr>
<tr>
<td></td>
<td>14 January and 4 February 2003—no reference.</td>
</tr>
<tr>
<td>18–Feb–03</td>
<td>Reference to progress on offence scheme; visit to examine the NSW Child Protection Register.</td>
</tr>
<tr>
<td></td>
<td>15 March—no reference</td>
</tr>
<tr>
<td>15–Apr–03</td>
<td>Need to revise project approach and Plan based on lessons learned from MNPP and tighten the plan on progress so far. Revision to be undertaken with jurisdictions and complete by end of April 03. Looking to deliver NCSOS (Jun 03) before MNPP in Nov 03. However, delivery of NCSOS is stated to be via the MNPP Pilot Project—links not clear.</td>
</tr>
<tr>
<td></td>
<td>13 May, 27 May and 10 June—no reference. No comment on the planned revision with jurisdictions.</td>
</tr>
<tr>
<td>24–Jun–03</td>
<td>Meeting cancelled, but papers detail NCSOS start date of May 02 and end date now Nov 04. A 15 month extension for NCSOS, no reasons listed.</td>
</tr>
<tr>
<td>8–Jul–03</td>
<td>Meeting cancelled.</td>
</tr>
<tr>
<td>19–Aug–03</td>
<td>Update for NCSOS not provided before meeting. Old papers left in show NCSOS start date of June 02 and planned end date of June 03 and project priority 4 of 5 in CPRS. ANCOR introduced—concept demonstrator and business case for ANCOR to be developed by 30 Sep 03.</td>
</tr>
<tr>
<td></td>
<td>2 September—no reference</td>
</tr>
<tr>
<td>30–Sep–03</td>
<td>NCSOS on hold—diverted to ANCOR. Concept demonstrator presentation to all CrimTrac staff. Working group to meet 2 Oct 03.</td>
</tr>
<tr>
<td>11–Nov–03</td>
<td>Last PCC meeting for analysis was held on 11 November 03. No reference.</td>
</tr>
</tbody>
</table>

Source: ANAO based on analysis of PCC meeting minutes and papers.
Analysis of this history shows that the NCSOS Project was considered by the PCC at irregular intervals and that actions forecast were not always followed up. Aside from the PCC requests for the NCSOS Project Brief and Project Plan to accommodate minor changes, the PCC appears to have provided little value-add to the project. No decisions appear to have been taken as a result of PCC meetings.

The ANAO acknowledges that NCSOS was replaced by the ANCOR Project in accordance with the APMC decision. However, a more consistent pattern was not evident for other CrimTrac projects.

The ANAO considered that the PCC was not effective in coordinating CrimTrac’s projects. Further, the ANAO found that, although the project reports were comprehensive, the templates encouraged much repetition of earlier data, and as a consequence it was difficult to track the changes in project milestones and costs and the reasons for these changes. This view is supported by a number of jurisdictions, who indicated in their survey returns that they found the project documentation difficult to follow and time consuming to analyse.

However, the ANAO notes that the PCC served a useful role in considering project management issues. It was responsible for initiating the procurement of PRINCEPlus, the software tool that supports PRINCE2, in November 2003. The PCC also initiated the provision of formal project management training for CrimTrac project and programme managers in early 2003.

CrimTrac previously had identified the coordination of its projects to be an issue and had commissioned a number of reviews into its project management methodology and practices.

In developing the CPPMF, CrimTrac commissioned a review by Tanner James Management Consultants to test the CPPMF for compliance with PRINCE2. The review identified some fundamental issues, such as flaws in the proposed use of the PCC, inadequate guidance on how the framework is to be applied, and confusion and overlap between the roles of the PCC and the programme managers.

The ANAO considers that, at the time of the audit, a number of these findings remained unresolved in CrimTrac’s project management framework. The ANAO noted that CrimTrac continues to try to improve its project management through initiatives such as the procurement of PRINCEPlus and commissioning a review of the MNPP Pilot Project. In the final PCC meeting minutes that the ANAO examined, there was discussion about the need to review the role of the PCC.
Conclusion regarding the role of the PCC

4.83 Notwithstanding these continuing initiatives, the ANAO concluded that the PCC was not effective in its role of providing operational and strategic coordination of the agency’s projects, and that CrimTrac would benefit from the establishment of an effective arrangement to coordinate its projects in a transparent and accountable manner.

Recommendation No.5

4.84 The ANAO recommends that CrimTrac establish an arrangement to more effectively coordinate its projects in a transparent and accountable manner.

CrimTrac response

4.85 Agree. Projects are transparent and accountable through the agency’s governance structure, however, it is recognised that the coordination of resources and integrated deliverables and dependencies requires a more effective mechanism.

4.86 CrimTrac believes that the rationale is sound but that supporting tools to reinforce the coordination of projects across the agency are required so that dependencies and available resources are readily identified and tracked.

Lack of timely provision of project management skills development

4.87 Effective project management requires those with management responsibilities to have relevant financial, personal and planning skills, as well as the necessary project content expertise. Structured skills development, usually in the form of training and development programmes, are an important way to facilitate effective project management that is consistent with corporate policies and is fundamental to achieving successful outcomes.

4.88 In an effort to increase project management competencies in CrimTrac, the PCC approved, in February 2003, that nominated CrimTrac project staff should receive formal training in the PRINCE2 project management methodology. The courses were four days in duration, with attendees undertaking an exam at the completion of the course.

4.89 In total, nine courses were undertaken between April and December 2003 with 23 CrimTrac staff members attending, including the Deputy CEO and the key programme managers. The ANAO was advised that all CrimTrac staff successfully passed the exam and thus qualified as PRINCE2 practitioners.
4.90 In addition to the formal PRINCE2 qualification, the PMO has also held monthly presentations to act as a refresher for staff on the PRINCE2 methodology.

4.91 However, in the absence of detailed guidance being contained in or supporting the CPPMF, and also the recognition that CrimTrac’s business success heavily relies on project management skills, the ANAO considers that earlier skills development training for CrimTrac staff would have been more appropriate for facilitating the efficiency and effectiveness of its operations.

**Conclusion regarding the efficiency and effectiveness of CrimTrac’s project management**

4.92 The ANAO concluded that CrimTrac has applied a project management methodology and framework. However, the ANAO concluded that the agency’s framework is not robust enough to be effective in a multi-agency project delivery environment. The ANAO has made recommendations aimed at strengthening the framework through:

- the provision of supporting policies and more detailed guidance, including the measurement of the full costs and benefits of its projects;
- the detailing of the roles and responsibilities of all parties involved in the projects and how these should interact;
- better defining the roles and responsibilities of the agency and jurisdiction project managers; and
- the establishment of the means to effectively coordinate its projects in a transparent and accountable manner.
5. IT Security

This chapter examines whether the data held by CrimTrac, or accessed through CrimTrac, for matching purposes is secure.

Introduction

5.1 CrimTrac’s projects are to provide the police with IT systems that facilitate information exchange on a nationwide basis. The information that is exchanged or accessed is sensitive in nature. Appropriate controls must be established to provide a secure environment for this to occur.

5.2 The ANAO examined CrimTrac’s IT environment in order to assess whether the data held by CrimTrac, or accessed through, CrimTrac is secure. The ANAO tested whether:

- CrimTrac has appropriate IT organisational planning;
- CrimTrac has appropriate security policies, plans and procedures and whether these are applied and monitored;
- the roles and responsibilities for the security of data are clear, including between CrimTrac and the jurisdictions; and
- adequate security awareness, education and training is provided.

5.3 The Protective Security Manual (PSM) and Australian Communications-Electronic Security Instruction 33 (ACSI33) were used as a framework for assessing the security controls surrounding the CrimTrac IT environment. These are the minimum standard required for government IT systems.

5.4 The audit was performed with a focus on the following areas of ACSI33:\n
- information Security Policy;
- allocation of security responsibilities;
- information security education and training;
- reporting of incidents;
- business continuity planning;
- change control; and
- compliance with security.

---

ACSI33 Handbook 4 Security Management. ANNEX A.
5.5 In addition to the above, the ANAO considered internal documentation, including the CrimTrac Security Policy (May 2002) and the IT Threat and Risk Assessment (TRA) (January 2002), in the overall assessment of NAFIS, NCIDD and the CrimTrac IT environment.

The CrimTrac IT environment

5.6 Currently, all CrimTrac systems operate across the CrimTrac network, which is provided by the AFP. Facilities support is provided by Defence Computing Bureau (DCB), which provides support for all mainframe operations and midrange operations, except NAFIS, which is housed in DCB, but is maintained separately. Facilities support includes ensuring computing equipment is maintained in working order, software is appropriately upgraded, and provision of IT support (such as problem resolution) and specific support requirements for CrimTrac applications (such as backup and batch processing requirements).

5.7 The PRS is a legacy mainframe based system that is currently one of the key business applications used by CrimTrac. A signed MOU and SLA exist between CrimTrac and the DCB for the provision of operational support for the PRS systems. At the time of the audit there was no date set for the decommissioning of these mainframe systems.

5.8 NAFIS, the first system deployed in April 2001, is a tailored vendor-provided product supplied by SAGEM, based on the application called MetaMorpho Automated Fingerprint Identification System (AFIS).

5.9 The other new technology implemented by CrimTrac is NCIDD, an in-house developed application that uses web-based browser technology.

5.10 The CPRS Capability Development Programme and ANCOR continue the model of the in-house developed web-based browser systems. NCHRC is a manual system that, at the time of the audit, was being re-engineered to a web-based system.

5.11 In addition to the deliverables under the IGA, CrimTrac also managed several IT infrastructure and common service IT systems and projects that included:

- network rationalisation programme (rationalisation of the CrimTrac Wide Area Network);
- enterprise architecture project (the CrimTrac underpinning enterprise architecture framework);

---

34 DCB does not provide facilities support for NAFIS, which is a custom designed system.
• searching and name matching project (common name matching protocols across systems using SSAName software);
• a new Financial Management Information System;
• storage area network to manage the increasing need for data storage;
• CrimTrac data security programme (common software to be applied across all systems, except NAFIS, eventually); and
• a messaging project.

5.12 The resources assigned to CrimTrac’s IT Services Group included a Director of IT and a team of 10 ongoing APS staff including software engineers, a technical writer, a project management officer, and three specialists. The IT Services Group also engaged eight contractors for the specific projects. CrimTrac has other IT staff reporting to the programme areas as required, for example the SAGEM contractors report directly to the NAFIS Programme Manager and the CPRS contractors report to the CPRS Capability Development Programme Manager. The Operations Support Group also employed an IT adviser and some business analysts.

5.13 In order to support so many diverse IT projects, the ANAO considers that sound IT governance and planning is required. In particular, given that different end users in the jurisdictions will use the different systems, it is also important that data security underpins each system and that the roles and responsibilities of all the programme managers, the system developers and the remote users are clear.

**IT organisational planning**

5.14 The ANAO examined CrimTrac’s IT planning at the organisational level. The ANAO also tested for the development and implementation of appropriate policies and procedures to support the IT planning.

5.15 Effective planning and organisation for IT is a critical element in ensuring IT functions and resources are effectively aligned, and will continue to align, with business directions. The business directions of CrimTrac are contained in the ‘CrimTrac Strategic Plan 2001–05’.

5.16 As CrimTrac operates in a complex environment, where its IT functions must effectively integrate with those of the eight jurisdictions that maintain independent technology and procedural environments, the need for effective planning is increased.

---

35 There are nine jurisdictions. However, eight jurisdictions are referred to because, from an IT perspective, the AFP and ACT police share the same network.
5.17 An overarching plan and approach is necessary to facilitate the implementation, performance monitoring, maintenance and update of technology planning, to assist CrimTrac to effectively achieve strategic targets and to continue to effectively provide for its clients. Such an approach should include processes for targeted and focused short term planning, progressing strategic goals, identifying priorities and project dependencies, and effectively allocating financial resources.

5.18 The ANAO found that CrimTrac had included the identification of IT related strategies in the CrimTrac Strategic Plan. CrimTrac also initiated a number of projects designed to deliver an overall IT architectural framework and a range of supporting common services.

5.19 The ANAO examined the two areas of the Strategic Plan that were relevant to data security, specifically Business Continuity and Information Security.

5.20 The ANAO found that of the four strategies detailed for Business Continuity, none of the four was fully implemented. Of the nine strategies for Information Security, four were relevant to data security, and the other five related to the privacy of information. Of the four information security strategies, the ANAO found that two were fully implemented, and the other two were partially implemented. Table 5.1 shows the strategies and their implementation status.

Table 5.1
CrimTrac strategies relating to data security

<table>
<thead>
<tr>
<th>Business Continuity</th>
<th>Information Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop and publish, in consultation with users, a Disaster Recovery Plan and Business Continuity Plan.</td>
<td>Conduct security awareness training for all staff, contractors and consultants.</td>
</tr>
<tr>
<td>Procure redundant services or equipment to cater for higher probability risks.</td>
<td>Develop and implement a Security Risk Management Plan.</td>
</tr>
<tr>
<td>Develop and implement an IT Strategic Plan.</td>
<td>Ensure that communication networks operate across secure lines and with encryption of data where appropriate.</td>
</tr>
<tr>
<td>Develop SLAs with service providers that ensure appropriate levels of disaster recovery and business continuity.</td>
<td>Implement access controls, authentication and audit logs.</td>
</tr>
</tbody>
</table>

Note: The shaded strategies are still to be fully implemented.


Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

5.21 At the time of the audit, CrimTrac did not have a formalised BCP or DRP. The ANAO noted that the importance of having such plans in place was
drawn to CrimTrac’s attention by the ANAO financial statement auditors in 2000–01 and in an internal audit report.

5.22 The internal audit report, that was in draft form at the time of the ANAO audit, found that:

There is currently no Business Continuity Plan (BCP) in place to ensure the ongoing availability of CrimTrac services to clients.

At the time of the review the CrimTrac Strategic Support and Communications Group are undertaking to develop a Business Continuity Plan for CrimTrac. Draft procedures have been developed and the Board will be considering the associated investment to support these procedures in the September 2003 Board meeting.

5.23 The ANAO noted that in the September meeting the BoM resolved that CrimTrac should produce detailed business continuity and disaster recovery options for the next BoM meeting, having regard to existing arrangements in place as part of the service agreements with the DCB and the AFP.

5.24 CrimTrac has identified a funding shortfall in the order of $10 million needed to establish a business continuity and disaster recovery capability. At the time of the audit, CrimTrac was considering options for funding these capabilities.

5.25 The ANAO considers that better practice is to include business continuity and disaster recovery planning as part of the systems development. The ANAO noted the co-location of many of CrimTrac’s key hardware, and further noted CrimTrac’s advice that it would take in the order of six months to rebuild NAFIS in the event of a disaster.

5.26 The ANAO noted that the staffing structure in the IT Services Group would have allowed only limited capacity to undertake these tasks. The ANAO further noted that CrimTrac recommended to the BoM in September 2003 that ‘business continuity planning be made a requirement on all current and future projects’.36

Conclusion regarding BCP and DRP

5.27 The ANAO concluded that CrimTrac, at some three years after the agency’s establishment, should formalise its BCP and DRP and procedures as a matter of priority. This will require the allocation of appropriate resources and the development of appropriate capabilities.

Recommendation No.6

5.28 The ANAO recommends that CrimTrac develop its Business Continuity Plan and Disaster Recovery Plan and accompanying procedures.

*CrimTrac response*

5.29 Agree. The development of plans are recognised as a priority.

IT Strategic Plan

5.30 The ANAO found that CrimTrac had yet to develop an overarching strategic plan for its IT function. CrimTrac advised the ANAO that it had commenced work on an overall IT Strategic Plan, but that resource constraints in the IT Services Group had prevented the Plan from being finalised.

5.31 The ANAO found that CrimTrac had articulated a strategic vision for its IT infrastructure, but that many of the components of this vision were yet to be addressed. While a number of projects were underway, there remained no overall plan on how to coordinate the IT goals and strategies.

5.32 The need for an IT Strategic Plan was raised in the management letters accompanying the ANAO financial statement audits for 2000–01, 2001–02 and 2002–03. For each year, the recommendation was: ‘as CrimTrac’s operations are extremely reliant on its IT systems it is recommended that a detailed IT Strategic Plan be formally developed and implemented as a matter of urgency’.

5.33 CrimTrac’s management agreed with the recommendation each year, and in 2002–03 advised that the IT Strategic Plan was being drafted.

5.34 The ANAO found that one of the consequences of not having a formal and approved IT Strategic Plan was that the planned architectural framework had not been fully developed and implemented. The resultant impact on CrimTrac’s data security policies and procedures is significant.

5.35 CrimTrac divided its IT framework into four domains to effectively plan and manage:

- **Information**—the use of information in CrimTrac’s care;
- **Application**—the technologies employed for developing and delivering CrimTrac systems for a range of business purposes;
- **Middleware**—the technologies employed for allowing the implementation of differing applications into varying technology environments maintained by jurisdictions; and

---

37 CrimTrac IT Architecture Version 1.1 (Common Services Model).
• **Security**—the security risks of the information processed and the security standards required to meet the needs of data owners and other stakeholders.

5.36 The ANAO found that the planned security architecture was comprehensive and, if fully and appropriately implemented, would provide the foundation for a strong security environment within CrimTrac.

5.37 The ANAO acknowledges that CrimTrac endeavoured to implement its architecture domains with limited resources and while facing significant pressures to deliver the operational systems required under the IGA. However, these pressures have impeded the agency from effectively planning and implementing the desired IT architecture and governance environment, as a first step, in accordance with better practice.

5.38 CrimTrac prepared a business case for the BoM meeting of February 2004 seeking the allocation of additional resources to the IT Services Group to assist it to address the need for an IT Strategic Plan and to progress the architecture framework.

**Conclusion regarding the IT Strategic Plan**

5.39 The ANAO concluded that CrimTrac should finalise its IT Strategic Plan as the critical foundation for the ensuing architecture and security framework that it needs to effectively integrate security into its business operations.

**Recommendation No.7**

5.40 The ANAO recommends that CrimTrac establish an IT Strategic Plan that addresses, plans and coordinates the use of IT as a foundation to support all CrimTrac’s business objectives. The IT Strategic Plan should be complemented by appropriate IT operational and business plans.

*CrimTrac response*

5.41 Agree.

**IT Security Policy, System Security Plans and procedures**

5.42 In forming an opinion whether the data CrimTrac either holds or accesses for matching purposes is secure, the ANAO examined CrimTrac’s IT policies and procedures for compliance with the PSM and ACSI33. These documents outline the security planning requirements that must be established to ensure appropriate security management.

5.43 The ANAO first examined whether CrimTrac had developed the required IT Security Policy, System Security Plans and corresponding system security procedures. The ANAO then tested CrimTrac’s compliance with its IT
policies and procedures in practice through a review of the NAFIS and NCIDD systems.

**Security Policy and System Security Plans**

5.44 For managing security overall, the PSM requires agencies to ‘develop and implement an agency Security Plan that is appropriate to the agency’s functions and the security risks that it faces’. The Security Plan needs to be based upon appropriate risk management practices.

5.45 The PSM provides a guide for the preparation of an agency Security Plan. The PSM suggests that the Security Plan (or policy) should include a statement of purpose that ‘makes explicit the relationship between agency security practices and the corporate plans and business objectives’. It further suggests that the Plan details the security environment by providing a summary of the threat assessment and the agency’s current exposure.

5.46 An IT Threat and Risk Assessment (TRA) was completed for CrimTrac in January 2002. This was limited in scope to consider high-level risks to the NCIDD, NAFIS, CPRS and PRS systems, as well as the CrimTrac Local Area Network.

5.47 Following from the TRA, CrimTrac developed an overall Security Policy that was released in May 2002. The Security Policy outlines a range of policy and procedural requirements for securing CrimTrac systems.

5.48 In accordance with better practice, an agency’s Security Policy should be based on a risk management approach and should directly stem from the required risk management controls identified in the TRA. However, the ANAO found the link between the results of the TRA and the policies and processes mandated in the Security Policy to be unclear. For example, there was no section in the Security Policy that detailed the agency specific risks that had been identified during the TRA, and no subsequent references within the Security Policy as to how these risks were to be mitigated.

5.49 This issue was also identified by CrimTrac’s internal auditors in their audit of IT security. CrimTrac advised that it is taking steps to implement the security architecture, and one of the steps has been to engage an external consultant to undertake a more detailed TRA and to then develop an improved Security Policy.

---


39 ibid. B:4.8,4.9.

5.50 The ANAO noted the work in progress, but also considers that the TRA and subsequent IT Security Policy would have benefited from the prior development of an IT Strategic Plan, as the basis for better identification of the strategic risks and the policies required to mitigate them. CrimTrac should progress its IT Strategic Plan prior to developing and implementing the supporting policies and plans. The ANAO further considers that CrimTrac should also develop an agency IT Security Plan as the means for implementing the Security Policy.

Conclusion regarding Security Policy and System Security Plans

5.51 The ANAO concluded that, overall, the existing CrimTrac Security Policy was generally consistent with the requirements under the PSM and ACSI33. However, the ANAO also concluded that its links to appropriate TRAs was insufficient, and, as a consequence, the procedural environment to ensure the protection of data was weakened. The work in progress at the time of the audit should assist CrimTrac to address this weakness.

5.52 The ANAO further concluded that CrimTrac would benefit from greater coordination of the development of its various IT security plans, policies and procedures, to ensure greater consistency between these plans, and to minimise the risks of gaps in the agency’s approach to the management of the security of its data and systems.

Implications for existing systems

5.53 Under the CrimTrac Security Policy of May 2002, Section—13.1 New Projects, new projects must have a TRA and a Security Plan, as follows:

...Project Managers are to ensure that:

- a TRA is conducted and appropriate security countermeasures formulated;
- a security plan is implemented as part of the project plan.

The Project Manager is to ensure that protective and IT security countermeasures (including privacy, access and audit requirements), are defined as part of the overall system requirements documentation and the subsequent System Security Plan.

5.54 NAFIS and NCIDD were developed in early 2001, some twelve months prior to the development of the CrimTrac Security Policy. The ANAO found that CrimTrac had not aligned the security framework for these systems with the Security Policy. Appropriate TRAs were not performed for either NAFIS or NCIDD during the design and development of these systems, and accordingly, System Security Plans were also not developed for either system.

5.55 However, NAFIS and NCIDD were included in the overall TRA completed in January 2002. A gap analysis was undertaken for NAFIS between
the security controls implemented and those required by the subsequent CrimTrac Security Policy. The ANAO was advised that, at the time of the audit, the gaps had not yet been addressed. The ANAO was further advised that, because NAFIS is a vendor provided product, addressing some of the gaps would be complex and expensive.

5.56 The ANAO noted that, in late 2003, CrimTrac commissioned a consultant to perform detailed TRAs for both systems as a component of the security architecture implementation projects being undertaken.

5.57 Additionally, the ANAO found that NCIDD did not, as at 31 December 2003, have a formal security classification assigned to the data or system. The PSM requires official information to be risk assessed and a security classification assigned based upon the consequences of unauthorised access to the information. The PSM further identifies minimum standards that must be applied for securing information at the various classification levels.

5.58 Without first identifying the security classification of NCIDD, it is difficult for CrimTrac to be sure the information is appropriately protected. Although the NCIDD was not yet fully deployed, the data from two States had been uploaded and the ANAO was advised that more data was to be loaded in early 2004.

5.59 The TRA that was in progress at the time of the audit included data classification exercises to formalise the security classifications of the systems and data. At the time of the audit, CrimTrac was expecting the outcome of the classification of NCIDD.

5.60 The ANAO further notes that, for systems managing classified information, the PSM recommends the employment of a third, preferably independent, party to review the completeness and effectiveness of the security controls implemented and to certify the system to the intended security classification level. Such certification can be performed by the Defence Signals Directorate (DSD) or via DSD-approved organisations. CrimTrac advised it had engaged an external consultant to perform a review of the data classification. The ANAO notes that this was CrimTrac’s preferred supplier of services and IT expertise.

5.61 Given the priority of security in CrimTrac operations to jurisdictions, the particularly sensitive nature of the data maintained, and the limited security controls currently in place over the systems reviewed, the ANAO suggests that CrimTrac continue to employ an independent assessor to undertake post-implementation and certification reviews of all future CrimTrac systems prior to deployment to the jurisdictions. Ideally, the

41 ibid. C:7.28.
assessor should be an accredited under the Infosec-Registered Assessor Programme (I-RAP) so that the system being assessed can be certified as meeting the standards set out in the PSM.

Conclusion regarding implications for existing systems

5.62 The ANAO concluded that there is scope for CrimTrac to better align the security framework for its existing systems with its Security Policy, with particular reference to the development of specific System Security Plans and accompanying procedures.

Compliance with existing security policies and procedures

5.63 The ANAO also examined NAFIS and NCIDD for compliance with the operational, day-to-day security procedures as outlined in CrimTrac’s Security Policy of May 2002. The ANAO tested for operational security requirements that are mandated under the PSM and the ACSI33 and that are expected to be present in Australian Government IT systems.

NAFIS

5.64 The NAFIS system is a client/server architecture that is specifically designed for a multi-jurisdictional environment. Physically, it consists of one central site, remote jurisdictional sites and multiple remote workstations at the jurisdictions.

5.65 The central site contains the permanent or archive database and the matcher repository, and these are located at DCB in Deakin. There are 128 servers located at DCB that support the central site.

5.66 Access to NAFIS workstations is secured via two levels of security. The first level of security is via a Windows NT session logon. The next level is provided via the NAFIS application security. The same person account name for Windows NT is also used for the NAFIS application logon, which guarantees traceability.

5.67 NAFIS has its own systems administration functionality, which allows the administrators to give users access to defined user profiles in accordance with the NAFIS User Access Overview. Systems administration is split between CrimTrac and the jurisdictions, with each jurisdiction having its own administrator. CrimTrac NAFIS administrators set up all new users. However, it is the responsibility of jurisdiction administrators to lock or unlock access depending on users’ movements.

5.68 Logging of users’ access is performed at the application and database levels. The CrimTrac NAFIS Programme Manager performs reviews of logging
information and the results are forwarded to jurisdictional systems administrators on a regular basis.

5.69 The results of the ANAO testing of NAFIS are shown in Table 5.2.

**Table 5.2**

<table>
<thead>
<tr>
<th>Test</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random sample of users to ensure that users were duly authorised and access was commensurate with role undertaken by the user.</td>
<td>Sample of 30 tested. 30 out of 30 access granted was appropriate to the role of the user. Only five of the 30 authorisation forms had been forwarded to the NAFIS Programme Manager. CrimTrac advised the missing forms are possibly due to a bulk upload of users when NAFIS was first implemented. The ANAO notes that this was in 2001. <strong>Overall: Not fully compliant.</strong></td>
</tr>
<tr>
<td>Review of data logging processes, and evidence that logging is reviewed on a timely basis.</td>
<td>Data logging found to be comprehensive. NAFIS Programme Manager emails the results of logging to jurisdiction administration staff monthly. ANAO notes no formal requirement for jurisdictions to respond and thus not possible to determine if jurisdictions had reviewed data, or if any issues had been addressed. <strong>Overall: Not fully compliant.</strong></td>
</tr>
<tr>
<td>Review of the enforcement of password settings and whether this is consistent with overall CrimTrac Security Policy.</td>
<td>Security policy states last 10 passwords may not be used. ANAO found NAFIS does not have the functionality to provide password history. <strong>Overall: Not fully compliant.</strong></td>
</tr>
<tr>
<td>Review of system administration functions and observation of functionality provided by the system.</td>
<td>At the time of the audit, there was no segregation between security administration functions used by jurisdictions and other administration functions used centrally by CrimTrac. CrimTrac has addressed this issue. <strong>Overall: Compliant.</strong></td>
</tr>
<tr>
<td>Review of user access profiles and whether these profiles are adequate given the current operations.</td>
<td>Some access profiles need reviewing. CrimTrac advised this was in progress. <strong>Overall: Not compliant. Under review.</strong></td>
</tr>
<tr>
<td>Review of change management procedures.</td>
<td>Changes reviewed and approved by NAFIS UAG and signed off by NAFIS Programme Manager. <strong>Overall: Compliant.</strong></td>
</tr>
</tbody>
</table>

Source: ANAO analysis based on CrimTrac data.
5.70 The ANAO concluded that the results of the testing show that NAFIS is not compliant with the CrimTrac Security Policy or the system access requirements under the PSM and ACSI33. The existing controls consequently require some improvement.

**NCIDD**

5.71 NCIDD is an in-house developed product that CrimTrac designed and developed in conjunction with Borland Enterprises.

5.72 The workstations in each jurisdictional forensic laboratory are connected to the NCIDD central server located in Canberra, via a dedicated, secure and encrypted network. The network is managed by the AFP.

5.73 The NCIDD contains:

- an application for batch uploading records to the central database;
- an application to add and match records to the central database; and
- a web-based browser to view matched results.

5.74 The central NCIDD database and the NCIDD servers are currently located at DCB in Deakin.

5.75 Access to NCIDD is secured via Windows NT session logon to the NCIDD terminal and then by NCIDD application access security. The same user account name is used for both Windows NT and NCIDD application logon.

5.76 The results of the ANAO testing on NCIDD are show in Table 5.3.
Table 5.3  
Results of NCIDD testing

<table>
<thead>
<tr>
<th>Test</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random sample of users to ensure that users were duly authorised and access was commensurate with role undertaken by the user.</td>
<td>At the time of the audit, no sample was tested as there were no access approval forms for jurisdiction users with data loaded. System not fully deployed. Subsequently, an access approval form has been developed. Overall: Not compliant. CrimTrac subsequently developed access approval forms, and these are used for new users.</td>
</tr>
<tr>
<td>Review of data logging processes, and evidence that logging is reviewed on a timely basis.</td>
<td>Logging processes found to be comprehensive and compliant with Security Policy. However, no formal plans for monitoring of logging and no filtering tool in place to allow monitoring by jurisdictions. Overall: Not fully compliant.</td>
</tr>
<tr>
<td>Review of the enforcement of password settings and whether this is consistent with overall CrimTrac Security Policy.</td>
<td>No functionality for evidence of password settings. Also no capacity to disable access, to change passwords or restrict passwords. Overall: Not compliant.</td>
</tr>
<tr>
<td>Review of system administration functions and observation of functionality provided by the system.</td>
<td>No segregation in place to separate security administration, security set-up, database administration and development. Overall: Not compliant.</td>
</tr>
<tr>
<td>Review of user access profiles and whether these profiles are adequate given the current operations.</td>
<td>At the time of the audit, no sample was tested as there were no access approval forms for jurisdiction users with data loaded. System not fully deployed. Subsequently, access approval forms have been developed. Overall: Not compliant.</td>
</tr>
<tr>
<td>Review of change management procedures.</td>
<td>At the time of the audit no change management procedures developed for NCIDD. CrimTrac is developing procedures. Overall: Not compliant. CrimTrac is developing procedures.</td>
</tr>
</tbody>
</table>

Source: ANAO analysis based on CrimTrac data.

5.77 The ANAO notes that NCIDD is yet to be operationally deployed, and data from all jurisdictions is yet to be loaded. However, CrimTrac advised that the system was fully developed and ready for data to be loaded.

5.78 The ANAO found that the NCIDD application security did not reflect the CrimTrac Security Policy. In addition, security administration functionality was yet to be developed for the system. At the time of the audit, user and security management was required to be undertaken by NCIDD developers through programmatic modifications to the system.

5.79 There was also yet to be a formal structure for security administration and the division of responsibilities between CrimTrac and jurisdictions established to manage the ongoing security of the system.
5.80 The ANAO concluded that the security of the NCIDD system was not complete. CrimTrac advised that this had been delayed pending the implementation of the CrimTrac security domain under its architecture framework. As noted earlier, constraints imposed on resources in the IT Services Group contributed to this outcome.

Conclusion regarding compliance with existing security policies and procedures

5.81 The ANAO concluded that neither NAFIS nor NCIDD were compliant with the CrimTrac Security Policy or the system access and security requirements under the PSM and ACSI33. The existing controls in place surrounding NCIDD and NAFIS require further improvement in order to adequately ensure data held and accessed for matching purposes is secure.

5.82 The ANAO further concluded that this may be a result of the absence of a coordinated and linked series of IT Security Plans within the CrimTrac agency, as well as the incomplete implementation of the security domain under the agency enterprise architecture framework.

Recommendation No.8

5.83 The ANAO recommends that CrimTrac, in consultation with its partners under the Inter-Governmental Agreement, develop an integrated approach to the management of data and system security across the agency. The approach should include developing:

(a) the full set of system security plans; and

(b) monitoring and evaluation mechanisms to ensure the compliance of each system and its users with the specified system security procedures.

CrimTrac response

5.84 Agree. The extensive security and audit capabilities of the PRS and NAFIS will be extended to all IT applications as they are brought online. This is reflected in the CrimTrac Enterprise Architecture framework.

5.85 The PRS is compliant, having been established for some time. System activity logs are kept indefinitely for audit purposes as required. A secure network exists. The NAFIS is a stand-alone system, with fully functional security. NCIDD is on a mid-range platform, which will be used for the new systems being developed, and these are evolving the required security procedures.
Clarity of data security roles and responsibilities

5.86 CrimTrac’s operating environment is complex, involving the exchange and matching of data across the Australian Government and each police jurisdiction in Australia. Within each jurisdiction there may be many users of the various CrimTrac systems.

5.87 The users of CrimTrac systems are law enforcement officers, health officials, forensic scientists or unsworn police staff. In addition, the data is only accessed, matched and released for law enforcement purposes. The ANAO considers that it is nonetheless important that the responsibility for the security of the systems and the data contained in these systems is clear. All users should be aware of the security requirements associated with the data they access.

5.88 Additionally, CrimTrac relies upon a range of suppliers of services and contractors who should also be aware of their security obligations for the CrimTrac systems they are associated with.

Agreed roles and responsibilities with jurisdictions

5.89 A key component of effective IT service delivery to clients is a clear understanding of the level of service that is to be provided. This is often agreed and defined through an MOU and/or SLA.

5.90 Within the CrimTrac Security Policy there is an expectation that MOU and SLAs will be in place between CrimTrac and external organisations, including the police jurisdictions, in order to enforce the Security Policy at the system user level.

5.91 Under the CrimTrac Security Policy–9.2 Data Security:

...CrimTrac must establish a Memorandum of Understanding (MOU) with the relevant party before inter-jurisdictional, Law Enforcement Agency and Accredited Agency connections are implemented.

5.92 The policy further states that all MOU dealing with the handling of the CrimTrac information by law enforcement agencies and accredited agencies (for the NCHRC), are to include a special clause that allows CrimTrac to audit controls used for these information-handling activities, and to specify the ways in which its information is to be protected.

5.93 However, the ANAO found that MOU had not been formally entered into with the police jurisdictions as users for NAFIS, and MOU were being progressed for NCIDD.

5.94 The ANAO found the content of the NCIDD MOU that had been finalised to date provided CrimTrac with the right to audit the management and use of these systems in jurisdictions, in accordance with CrimTrac’s
Security Policy. However, these MOU did not adequately address the required security procedures to be employed to manage system and data security.

5.95 As at December 2003, MOU had been developed and signed for the sharing of DNA data relating to the operation of NCIDD for New South Wales, Queensland and Victoria.

5.96 The MOU with the Queensland Police Service (QPS) outlines that CrimTrac is responsible for:

- developing and implementing, following consultation with the QPS and the Australian Police Services, security arrangement and audit protocols for the NCIDD to prevent unauthorised access, disclosure and corruption of information. This includes the implementation of access controls for all personnel accessing the NCIDD and the management of audit logs of access to the NCIDD and immediately reporting any security or confidentiality breaches of NCIDD to QPS.

5.97 The ANAO noted that the MOU for NCIDD do not place any requirement on the jurisdictions to enforce the CrimTrac Security Policy at the system user level as required under the CrimTrac Security Policy. The ANAO further noted that the MOU had been developed in advance of the formal security classification being assigned to NCIDD, which would make the specification of the required security protocols difficult.

5.98 CrimTrac advised that, on the advice of the CrimTrac Agency Security Adviser (ASA), it was considering the establishment of an overarching MOU for all security relationships between CrimTrac and the jurisdictions.

5.99 The ANAO considers that the establishment of such an overarching MOU would have considerable advantages in allowing for the clarification of, and agreement to, the respective ownership, roles and responsibilities relating to the systems and the data as it passes between them.

5.100 Jurisdictions, in their responses to the ANAO survey, indicated that they held few concerns relating to the adequacy of the security of the data and systems. However, responses reflected a lack of clarity about ownership of the data and the accompanying responsibility for it. Responses to the questions regarding who held the responsibility for the data and for the data systems varied, and included:

- Jurisdictions for data transferred and received—CrimTrac while it is on the lines.
- Jurisdictions, CrimTrac is only a custodian.
- Jurisdictions—this can’t be delegated.
- SAGEM, under CrimTrac (for NAFIS).
- CrimTrac and jurisdictions as joint custodians.
• CrimTrac.
• This has not been discussed (for new systems).

5.101 The ANAO considers that the roles and responsibilities for data security between CrimTrac and the jurisdictions are not consistently defined and understood by all the partners.

Conclusion on agreed roles and responsibilities with jurisdictions

5.102 The ANAO concluded that there is scope for CrimTrac to better define the role of the agency and that of the jurisdictions with respect to data and system security. In the absence of an agreed understanding of responsibilities there is a risk that inconsistent security protocols may be applied. There is a further risk that, if the ownership of the systems and data is unclear, adequate monitoring will not be conducted and breaches may occur undetected.

5.103 The ANAO further concluded that CrimTrac should seek to establish formal agreements with the jurisdictions that cover the ownership of the data and systems and assign responsibilities for the security of these data and systems accordingly.

Recommendation No.9

5.104 The ANAO recommends, for the purposes of maintaining consistency of data security, that CrimTrac seek to establish Memoranda of Understanding with the jurisdictions that agree the security standards to be applied and assign responsibility for monitoring compliance.

CrimTrac response

5.105 Agree. Existing systems (PRS and NAFIS) have robust security policies and procedures and these standards will be built into all new agreements as new technologies are introduced, in conjunction with jurisdictional partners. The NCIDD MOUs between CrimTrac and each jurisdiction include specific schedules on security of data and the MOU being prepared for MNPP also includes specific statements on the security standards to be applied and the responsibilities of each party for monitoring compliance.

Agreed roles and responsibilities with service providers

5.106 In order to effectively deliver systems to support the police jurisdictions, CrimTrac must rely on providers for various components of its IT infrastructure, including the AFP and the DCB. The ANAO examined the agreements in place to formalise the responsibilities for the provision of these services and to define the agreed standard of service.

5.107 The ANAO found that there was a signed MOU and SLA with DCB, which provides operational support for PRS. The PRS are hosted on a
mainframe that will be decommissioned once the CPRS suite of new projects is delivered.

5.108 The ANAO found evidence of a draft, unsigned MOU between CrimTrac and AFP for the provision of Network Services dated 20 July 2000. It was drawn to CrimTrac’s attention as part of the ANAO financial statements audit for 2002–03 that this MOU was not signed.

5.109 The ANAO further found that the MOU and SLA with DCB were not up to date with the operational requirements for NCIDD and NAFIS. CrimTrac advised that a project is underway to address this gap. No date was provided for when this would be completed.

5.110 In making these observations, the ANAO noted that a number of compensating factors exist to mitigate risk, including the limited access of the data users, the certification of the AFP network to Highly Protected, and the certification of the DCB to Confidential.

5.111 However, the ANAO concluded that many of the factors required to ensure appropriate security and security management remain outstanding, including an absence of agreed standards or processes for infrastructure availability, disaster recovery or incident response and reporting. The latter represents a significant risk, especially in the absence of formal CrimTrac BCP and DRP and a recovery capability.

5.112 The agreed arrangements with providers should include:

- clear definition of the security requirements of CrimTrac;
- clear definition of the division of roles and responsibilities for security between CrimTrac and the provider;
- availability requirements, based on analysis of the requirements of CrimTrac customers;
- procedures for incident response, reporting, backup and recovery; and
- disaster recovery arrangements, procedures and timeframes—consistent with CrimTrac’s BCP and DRP requirements.

5.113 ANAO was advised that, in a recent incident, NAFIS and other CrimTrac systems suffered an outage of four days in duration.

Conclusion regarding the agreed roles and responsibilities with service providers

5.114 The ANAO concluded that CrimTrac should ensure that its formal agreements with its service providers are up to date, finalised and appropriately signed off.
Recommendation No.10

5.115 The ANAO recommends that CrimTrac review its formal agreements with its service providers to make sure that these agreements are up to date, finalised and appropriately signed off.

CrimTrac response

5.116 Agree. The NAFIS MOUs are up to date as of April 2004. The new MOUs and SLAs for DCB and the AFP have been drafted since the ANAO performance audit began and should be completed by June 2004.

Security awareness, education and training

5.117 Once the ownership has been assigned to the data and systems, and the higher-level roles and responsibilities defined, it is important that the daily users understand the agreed requirements. For any security management environment to be effective, all those involved need to be aware of, and sufficiently educated in, the concepts, policies and procedures in force to provide for security.

5.118 The PSM requires that agency security education and awareness activities are undertaken for all employees upon induction and at appropriate intervals during the course of employment. The ANAO found that this requirement had been reflected within the CrimTrac Security Policy, which requires security awareness training, including IT security, to be provided to new staff and contractors and for updated training to be delivered annually for all staff.

5.119 The ANAO was advised that staff undertake an online security awareness course and a test provided by the Protective Security Coordination Centre (PSCC). However, in discussions with staff during the audit, the ANAO noted a varying level of awareness of the CrimTrac Security Policy and associated security.

5.120 The draft internal audit report into IT security found that, although CrimTrac had developed induction materials applicable to security, there was no provision for annual update training.

5.121 The ANAO considered that there is scope for more consistency and rigour in CrimTrac’s conduct of security training, in particular the conduct of update training.

5.122 The ANAO considers that system owners and system development staff have responsibilities for ensuring security in excess of those of general CrimTrac staff. The security training needs of such staff should be commensurate with these additional requirements.
5.123 The CrimTrac programme managers have a responsibility, together with the IT Services Group, for the effective management of the security of the system assigned to them and the data contained in it. As noted earlier, the existing systems developed by CrimTrac are not fully compliant with the minimum security requirements of CrimTrac’s Security Policy, nor Australian Government security policies as specified in the PSM and ACSI33.

5.124 The ANAO considered that CrimTrac would benefit from specific security training for its various programme managers and system development staff.

5.125 The CrimTrac Security Policy identifies the requirements for users to be made aware of, and to comply with, CrimTrac security requirements. The ANAO found that it was unclear whether CrimTrac had a role in the provision of security training to the jurisdictional users of its systems. There was no evidence of formal training having been conducted by CrimTrac, and in the absence of an MOU, there appeared to be no requirement for jurisdictions to conduct such training.

5.126 One way to improve or facilitate user awareness would be through online definition of the security standards and procedures to be applied. The ANAO found that the existing user documentation, screen displays and logon banners did not provide for a complete understanding of the security responsibilities and requirements of users accessing CrimTrac applications.

Conclusion regarding security awareness, education and training

5.127 Overall, the ANAO concluded that there was not an apparent targeted approach to the identification of security training requirements and the provision of appropriate training.

5.128 The ANAO further concluded that CrimTrac would benefit from the development of a more strategic and coordinated approach to the training of all those involved in its systems in relation to the security standards and procedures to be applied.

Recommendation No.11

5.129 The ANAO recommends that CrimTrac review its security training policies and procedures and develop a strategic approach to the training of all those involved in the development, management, support or use of its various systems.

CrimTrac response

5.130 Agree. The jurisdictions may, however, wish to retain control over the training of their users in relation to CrimTrac systems security requirements,
although CrimTrac provides general guidance in relation to these requirements.

**Conclusion regarding the security of data**

5.131 The ANAO has reported a number of findings relating to the controls and procedures in place to ensure the security of CrimTrac’s systems as well as the security of data it either holds, or accesses, for matching purposes. The ANAO notes that most of CrimTrac’s data is only accessible by police jurisdictions and that, to date, there have been no breaches or incidents of significance. However, as CrimTrac continues to build systems and to host increasing volumes of sensitive data, it is important that adequate controls are in place to protect the data.

5.132 The ANAO concluded that, overall, the existing CrimTrac Security Policy was generally consistent with the requirements under the PSM and ACSI33. However, the ANAO also concluded that its links to appropriate TRAs was insufficient, and, as a consequence, the procedural environment to ensure the protection of data was weakened. The work in progress at the time of the audit should assist CrimTrac to address this weakness.

5.133 CrimTrac would benefit from finalising the development of its various IT security policies, plans and procedures as well as implementing measures to ensure greater consistency between these plans. This would minimise the risks of gaps in the agency’s approach to the management of the security of its data and systems. CrimTrac should, as a matter of priority, finalise its IT Strategic Plan, Business Continuity Plan and Disaster Recovery Plan.

5.134 The ANAO further concluded that CrimTrac should establish formal agreements with the jurisdictions which cover the ownership of the data and systems and assign responsibilities for the security of these data and systems accordingly. Additionally, CrimTrac should ensure that its formal agreements with its service providers are up to date, finalised and appropriately signed off. The ANAO also concluded that CrimTrac take a more strategic approach to the security training of staff and users of its various systems.
The implementation of these strategies will assist CrimTrac to deliver a robust IT security environment that is appropriate for the management of sensitive data being held, accessed and matched to support Australia’s police jurisdictions.
Appendices
## Appendix 1: Survey Form—Views of CrimTrac

### PART A: Program Specific Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>NAFIS</th>
<th>NCIDD</th>
<th>NCSOS (now ANCOR)</th>
<th>CPRS Capability Development Program</th>
<th>Third party access NCHRC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Progress towards implementing the deliverables</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. What is the current status of this program/project?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Has the rate of progress been in accordance with the agency’s original expectations and planned milestones?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. What do you consider to be the major achievements for these programs? Are these in accordance with the original expectations of the program?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. What were the major challenges faced in the development of each of these programs? Did these impact on the timetable?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Project planning and management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Please describe how the agency addressed and managed these challenges?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. What are the ‘lessons learned’ if any, and how have these been incorporated into other current or future projects?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>NAFIS</td>
<td>NCIDD</td>
<td>NCSOS (now ANCOR)</td>
<td>CPRS Capability Development Program</td>
<td>Third party access NCHRC</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
<td>-------</td>
<td>-------------------</td>
<td>-------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>Progress towards implementing the deliverables</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Are there any other comments you would like to make about CrimTrac’s resourcing for these programs?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Do you believe the Commonwealth has received value for money for its contribution to the programs?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security of the data held or accessed for matching</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Who is responsible for the data and its security at the various stages of its matching processes for each program?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Similarly, who is responsible for the security of the data systems for each program?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. What are the risks / challenges facing the security of the data?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. How are the risks being managed?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. Do you have any concerns about the security of the data?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### PART B: CrimTrac Overview Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Do you believe that the role CrimTrac adopted has been, and continues to be, appropriate?</td>
<td></td>
</tr>
<tr>
<td>2. Are there any specific changes you would wish to make to CrimTrac’s role or the way the agency conducts its business?</td>
<td></td>
</tr>
<tr>
<td>3. Do you believe the Commonwealth has received value for money for its $50 million contribution?</td>
<td></td>
</tr>
<tr>
<td>4. Are there any comments you would like to make on CrimTrac’s profile within the ‘policing industry’?</td>
<td></td>
</tr>
<tr>
<td>5. Do you believe that CrimTrac is well positioned to aid nationwide policing into the future?</td>
<td></td>
</tr>
<tr>
<td>6. Do you believe that CrimTrac is well positioned to sustain itself financially into the future?</td>
<td></td>
</tr>
<tr>
<td>7. Generally, do you regard the CrimTrac initiative to be successful?</td>
<td></td>
</tr>
<tr>
<td>8. Are there any other comments you would like to make?</td>
<td></td>
</tr>
</tbody>
</table>
## Appendix 2: Survey Form—Views of the Police Jurisdictions

Completing jurisdiction:………………………………………………………………
Contact officer:……………………………………………………………………

### PART A: Program Specific Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>NAFIS</th>
<th>NCIDD</th>
<th>NCSOS (now ANCOR)</th>
<th>CPRS Capability Development Program</th>
<th>Third party access NCHRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. How would you describe the current status of this program/project?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Has the rate of progress been as planned / expected?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. What have CrimTrac's major achievements been for these programs?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. What were/are the major challenges faced in the development and implementation of these programs?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. What comments would you make about how CrimTrac addressed / managed these challenges?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. How do these programs add value to or benefit the work in the Jurisdictions?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. How would you describe CrimTrac’s consultative processes during the development of these programs?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. How responsive was CrimTrac to the needs of the Jurisdictions?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Question 9
Are there any particular ‘lessons learned’ from the development of these programs?

### Question 10
Who is responsible for the data and its security at the various stages of the matching processes?

### Question 11
Similarly, who is responsible for the security of the data systems?

### Question 12
Do you have any concerns about the security of the data?

### PART B: CrimTrac Overview Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Do you believe that the role adopted by CrimTrac has been, and continues to be, appropriate?</td>
<td></td>
</tr>
<tr>
<td>2. Are there any specific changes you would recommend to the way CrimTrac conducts its business?</td>
<td></td>
</tr>
<tr>
<td>3. Do you consider that CrimTrac has understood and accommodated the differing frameworks in, and requirements of, the individual Jurisdictions? If possible, please provide an example to support your answer.</td>
<td></td>
</tr>
<tr>
<td>4. Are there any comments you would like to make on CrimTrac’s profile within the ‘policing industry’?</td>
<td></td>
</tr>
<tr>
<td>5. Do you believe that CrimTrac is well positioned to service nationwide policing into the future? (For example, does it plan strategically to align itself with future needs?)</td>
<td></td>
</tr>
<tr>
<td>6. Do you believe that CrimTrac is well positioned to sustain itself financially into the future?</td>
<td></td>
</tr>
<tr>
<td>7. Generally, do you regard the CrimTrac initiative to be successful?</td>
<td></td>
</tr>
<tr>
<td>8. Are there any other comments you would like to make?</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 3: CrimTrac response

The CrimTrac Agency notes the key findings arising from the audit and observes that a reasonable balance has been struck between ANAO acknowledgment of several Agency successes since formal start-up in 2000, helpful suggestions for improvement of outcomes and performance, constructive criticism where it is warranted and identification of some key issues that have frustrated the Agency and affected its progress in producing the key deliverables specified in the IGA.

Comments on the NAFIS overlook a world first and the fact that the Australian NAFIS has been a point of reference for the UK, Canada, China, South Africa and the US since 2001 as they have sought to duplicate the functionality and crime-solving speed of its unique palm print database. The wisdom of Australian police having recorded and kept palm prints in hardcopy format over many years, and the ability to fully exploit this valuable information asset through the new NAFIS also warrants recognition.

CrimTrac believes that significant progress has been made during the first three years. The majority of funds allocated have be spent within this time. This has been achieved in a multi-jurisdictional policing environment where each new or improved system or service implemented by the CrimTrac Agency introduces business process change in the police jurisdictions. The degree of budget and human resource readiness to gear up for such change and the ability to allocate jurisdictional funding to facilitate such change within state and territory police budgets has been variable across police jurisdictions.

The CrimTrac Agency is capable of scaling up for rapid project delivery where there is early jurisdictional agreement on what is to be built. Such was the case with the ANCOR Project, which has progressed beyond concept development to “build” stage since the ANAO audit commenced and is on track for delivery and implementation by 1 September 2004. The Agency also reacted swiftly to design, deliver and implement the National Handgun Buyback Support System (NHBSS) which has underpinned efficiency, consistency and informing of the public during the COAG-initiated [Council of Attorneys-General] national handgun buyback in 2003 and 2004. Our achievement in reacting to the Bali disaster is also worthy of mention.

The NHBSS was an additional deliverable not identified in the IGA but broadly facilitated by means of Recital E to the IGA, which states that “the CrimTrac framework is intended to provide the means by which these components and other emerging policing requirements across jurisdictions can be considered and met as appropriate.”

As has proved to be the case with some CrimTrac systems and services, police jurisdictions have the option under the IGA of not participating in every
initiative and may withdraw from the entire IGA with due notice. Since the CrimTrac Agency does not have any overriding authority to command the immediate application of jurisdictional IT or policy resources to match those being applied centrally, the Agency has needed to be prudent and patient in drawing down and spending the $50 million of Commonwealth funds.

CrimTrac holds the view and expects that Australian police would agree, that significant progress has been made in the first three years, albeit without spending all of the funds originally allocated. The whole fund has, however, been carefully allocated to the complete span of IGA deliverables and it may transpire that the original $50 million is insufficient to achieve the delivery of all CrimTrac initiatives to every jurisdiction, to the depth and quality that is required, especially in the changed threat environment that has emerged since the IGA was signed in 2000.

Too much weight has been placed on the initial budget forward estimates of expenditure in relation to the $50 million. The actual spending pattern has not been contentious with the Department of Finance or with the Attorney-General’s Department and this indicates spending should not be used as a performance measure regarding CrimTrac’s progress. Pressure to spend would only encourage waste and poor fiscal decision-making.

With respect to the establishment of a “...framework for the timely resolution of key issues...” the CrimTrac Board of Management, at its February 2004 meeting, agreed with the recommendations of a report commissioned by the Board and prepared by the Police Commissioners Policy Advisory Group (PCPAG) on the future strategic direction of the CrimTrac Agency. (This report resulted from inter-jurisdictional consultations that included CrimTrac, in the latter half of 2003 and before the ANAO audit was announced.) The Board resolved to form a Strategic Issues Group, comprised of a senior police representative from each jurisdiction and a CrimTrac representative, to advise the Board on matters of strategic importance – the advice to cover policy, legal, forensics, finance, project management, operational and information technology issues. ANAO’s assertion that NCIDD has not been deployed is quite wrong. The system was built and delivered to agreed specification. The report acknowledges that there has been a delay in utilisation of the system for reasons beyond CrimTrac’s control although we have demonstrated effort to engage stakeholders and influence outcomes through our governance structure. The general conclusions that the Agency is responsible are difficult to comprehend.

For the future, the work of the SIG should assist the Agency in resolving “key issues that pose a risk to the CrimTrac Outcome, or to particular projects.” The Agency welcomes this decision and expects the first meeting of the SIG to occur in mid-May 2004. The CEO CrimTrac will be the Agency’s SIG
CrimTrac is committed to data security and agrees with the need to refine and strengthen its Security Policy, other plans and procedural environment to ensure continued vigilance over the protection of data. It should be acknowledged, however, that it is not just serendipitous that CrimTrac has successfully protected all data entrusted to it since 2000 and that there have been no information security breaches. Significant policy, procedural and IT measures are already in place and are being monitored to maintain the security of data entrusted to the CrimTrac Agency.

Police Reference Systems taken over from NEPI have had robust IT security since their implementation some years ago and continue to have this level of IT security; the NAFIS is a ‘stand-alone’ system with equally robust IT security and the current arrangements with the Defence Computing Bureau (threat risk assessments) and the Australian Federal Police (data encryption and protected network) are designed to ensure full security of data holdings.

The IT Security infrastructure for the existing systems and for those in development (CPRS, ANCOR) that will be deployed in the midrange computing environment, is being delivered to the highest appropriate security standard. Additional measures have been taken with NCIDD data to ensure that information relating to DNA cannot be used for any other purpose. Arrangements with DCB and the AFP will also be available for the new systems. CrimTrac plans to employ a dedicated IT Security Manager as soon as possible, with duties focussed on IT security for all CrimTrac systems.

In response to the problems experienced in estimating the costs of projects identified in the report CrimTrac has found that:

- Its systems are unique and without precedent;
- In the case of MNPP, the revision of estimates arose as the scope of the work became clearer. That project has highlighted that scoping activity is not a CrimTrac activity alone. There is significant input required from the jurisdictions.

CrimTrac is grateful for ANAO recognition that the Agency has experienced difficulty in deploying the NCIDD, due to legislative lags, and has felt frustrated in meeting the requirements of the IGA in this regard. Jurisdictional views, on the other hand, may well be that NCIDD development has been a case of “IT driving the business”, rather than the reverse. Although CrimTrac has acted vigorously to bring the matter to the attention of the appropriate bodies, this has not accelerated progress to any great degree and legal barriers to national operation of the NCIDD are being dissolved too slowly for comfort.
CrimTrac anticipates that the Strategic Issues Group (SIG) may assist the Board of Management in this area.

**Recommendation 1**

Agree. CrimTrac would prefer to have a set of guiding principles, as MOUs can be cumbersome and consensus has proven to be difficult and expensive to achieve. Jurisdictions may opt not to participate in all initiatives and are keen to preserve this right, as set out in the IGA.

**Recommendation 2**

Agree. CrimTrac notes ANAO’s acknowledgement that delays in legislative amendments are clearly beyond the scope of the CrimTrac Agency to resolve but that CrimTrac had made effort to influence the progression of legislation issues affecting NCIDD. This included escalation to the APMC in accordance with the governance defined in the IGA. CrimTrac is of the view that by using this established governance all stakeholders have been made well aware of NCIDD legislation issues.

**Recommendation 3**

Agree. CrimTrac recognises that effective project management is essential to its success and has taken a number of steps to improve its project management environment since 2000:

- It employs professional project managers;
- It has required all staff to attend the PRINCE2 foundation project management course (a 4-day intensive course conducted by fully accredited PRINCE2 training provider);
- PRINCE Plus is available online to all staff, enabling them to use all the templates with online help and system navigation;
- It employs an accredited PRINCE2 full-time Project Management Officer to provide expert advice to any agency personnel in the use of the methodology and to provide an independent source of scrutiny for particular projects;
- It has commissioned an external review of its project management to assess the areas in which this may be improved. Following the Board’s endorsement of recommendations of that review in February 2004, the Agency has acted to inculcate better project management and governance across all active projects.

The CPPMF is an evolving project management framework for the agency and is now more focussed on PRINCE2, which provides this guidance. The PRINCE2 is a proven internationally accepted methodology. Project templates include cost/benefit analysis, although many benefits from projects with
outcomes that are social in nature are often difficult to attribute or measure directly.

Experience has shown that CrimTrac projects involve significant project work in the jurisdictions as well as at CrimTrac.

Recommendation 4
Agree.

Recommendation 5
Agree. Projects are transparent and accountable through the agency’s governance structure, however, it is recognised that the coordination of resources and integrated deliverables and dependencies requires a more effective mechanism.

CrimTrac believes that the rationale is sound but that supporting tools to reinforce the coordination of projects across the agency are required so that dependencies and available resources are readily identified and tracked.

Recommendation 6
Agree. The development of plans are recognised as a priority.

Recommendation 7
Agree.

Recommendation 8
Agree. The extensive security and audit capabilities of the PRS and NAFIS will be extended to all IT applications as they are brought online. This is reflected in the CrimTrac Enterprise Architecture framework.

The PRS is compliant, having been established for some time. System activity logs are kept indefinitely for audit purposes as required. A secure network exists. The NAFIS is a stand-alone system, with fully functional security. NCIDD is on a mid-range platform, which will be used for the new systems being developed, and these are evolving the required security procedures.

Recommendation 9
Agree. Existing systems (PRS and NAFIS) have robust security policies and procedures and these standards will be built into all new agreements as new technologies are introduced, in conjunction with jurisdictional partners. The NCIDD MOUs between CrimTrac and each jurisdiction include specific schedules on security of data and the MOU being prepared for MNPP also includes specific statements on the security standards to be applied and the responsibilities of each party for monitoring compliance.
Recommendation 10

Agree. The NAFIS MOUs are up to date as of April 2004. The new MOUs and SLAs for DCB and the AFP have been drafted since the ANAO performance audit began and should be completed by June 2004.

Recommendation 11

Agree. The jurisdictions may, however, wish to retain control over the training of their users in relation to CrimTrac systems security requirements, although CrimTrac provides general guidance in relation to these requirements.
Appendix 4: Special interest party responses

AUDIT-IN-CONFIDENCE

Australian Government
Attorney-General's Department
Secretary

6 May 2004

Mr David Crossley
Executive Director
Performance Audit Services Group
ANAO
GPO Box 707
CANBERRA ACT 2601

Dear Mr Crossley

Performance audit: the implementation of CrimTrac

I acknowledge your letter dated 8 April 2004 inviting comments on the proposed audit report on the implementation of CrimTrac. I understand you have also invited comments from CrimTrac, the Australian Federal Police and other relevant jurisdictions.

The Department’s comments on relevant recommendations are provided at Attachment A. As your report acknowledges, the governance arrangements for the CrimTrac agency are complex, and its work program has been challenging. I am confident that, within these constraints, action taken to address issues raised by the ANAO will prove valuable in progressing the CrimTrac initiative.

Thank you for the opportunity to comment. The action officer for this matter is Anton Schneider who can be contacted on 6250 6778.

Yours sincerely

[Signature]

Robert Cornall
Secretary

---

The Australian Federal Police Service response includes comments from the ACT Police Service.
Proposed audit report—comments from Attorney-General’s Department

Recommendation No. 1

Agree in principle.

The governance arrangements for the CrimTrac agency reflect the important role that the States and Territories have in working in partnership with the Australian Government to set priorities for the agency that reflect national and jurisdictional policing needs and in overseeing and monitoring the work of CrimTrac.

The Australian Government’s $50m CrimTrac initiative, which was endorsed by the Australasian Police Ministers’ Council, set initial priorities for the agency. These were the replacement of the national fingerprint system, the establishment of a national DNA system and child sex offender system, and the provision of better access to operational information.

CrimTrac’s role is to provide and coordinate national operational policing information systems. It is not responsible for the necessary policy and legislative developments required to support provision of information to those systems. Those responsibilities rest with Commonwealth, State and Territory governments.

The Board of Management, which is responsible and accountable for the efficient and effective delivery of the CrimTrac initiative, has a membership that reflects the cooperative nature of the initiative. In addition to the Commonwealth member who was the inaugural Chair, two voting members appointed by APMC represent the larger jurisdictions, two voting members appointed by APMC represent the smaller jurisdictions and two non-voting members appointed by the Senior Officers’ Group of the APMC provide specialist advice on information technology and finance matters.

Under the direction of the Board, CrimTrac has established a national fingerprint system and a national DNA system. It is developing a national child sex offender register with a scheduled establishment date of 1 July 2004, and is piloting an initiative to improve access to operational information under its CrimTrac Police Reference System program. The focus of the Board and the agency has been on developing the systems approved as part of the CrimTrac initiative in priority order. In doing so, an individual Board member has taken responsibility for championing specific projects that require cross-jurisdictional support.

As the initiative moves towards developing the new systems to improve access to national operational policing information, it will be increasingly important that jurisdictions provide full cooperation and support by ensuring their jurisdictional priorities, particularly in the area of IT infrastructure development, reflect their support for CrimTrac’s national projects. The roles and responsibilities of the agency and all
AUDIT-IN-CONFIDENCE

Australian jurisdictions will need to be more clearly defined in relation to specific projects.

Recommendation 2
CrimTrac is an administrative agency and as such does not have the responsibility or authority itself to resolve inter-jurisdictional policy and legislative issues. CrimTrac provides regular progress reports to meetings of the APMC and its Senior Officer Group which, if required, identify policy issues that require resolution at Ministerial or government level. The Chief Executive Officer of CrimTrac also meets regularly with the Minister for Justice and Customs who has responsibility for CrimTrac as a Commonwealth Executive agency.

The cooperative nature of the CrimTrac initiative requires policy issues to be dealt with in the APMC forum. The work program for CrimTrac is extensive and requires strategic input from a wide range of stakeholders.

The utilisation of the national DNA system (NCIDD) required the development of model legislation to harmonise the collection and provision of DNA samples across jurisdictions. The legislative issues involved were complex and were discussed at meetings of Commonwealth, State and Territory officials, APMC, SCAG and the Council of Australian Governments (COAG). The passage of legislation necessary to ensure full operational status for systems such as the NCIDD requires consideration by APMC, the Standing Committee of Attorneys-General, and ultimately are matters for State and Territory Parliaments.

Recommendation 3, 4, 5,
Matter for CrimTrac.

Recommendation 6
Agree.

Recommendation 7
Agree.

Recommendation 8, 9
Matter for CrimTrac.

Recommendation 10
Agree.

Recommendation 11
Matter for CrimTrac.
Mr David Crossley  
Executive Director  
Performance Audit Services Group  
Australian National Audit Office  
GPO Box 707  
CANBERRA ACT 2601

Dear Mr Crossley

PERFORMANCE AUDIT: THE IMPLEMENTATION OF CRIMTRAC

Thank you for your letter of 8 April 2004 and accompany draft report regarding the Australian National Audit Office (ANAO) performance audit of the implementation of CrimTrac. New South Wales Police appreciates the opportunity to comment on the draft report and supports the draft recommendations in-principle.

Two factual errors in the draft report at paragraphs 2.40 and 2.99 have been drawn to my attention. The CrimTrac Agency will provide corrections in their agency response.

Of concern is paragraph 3.31 in which the ANAO draft report states that: "...the Police Commissioners do not appear to make decisions regarding the commitment of the jurisdictional resources necessary to make any systems or procedural changes in the jurisdictions".

I am advised that the ANAO survey form did not identify any specific questions of jurisdictions as to allocation of resources to meet local systems changes as a result of CrimTrac initiatives. New South Wales Police has established and resourced the CrimTrac Coordination Unit to address local procedural changes in response to CrimTrac systems. The organisation is also currently seeking funds through the usual budget process for system enhancements as part of the Australian National Child Offender Register (ANCOR) project.

I would appreciate the Auditor-General considering these comments before finalising the report.

Yours sincerely

K. E. Moroney  
Commissioner

Locked Bag 6102  Parramatta NSW 2124  
Tel (02) 8263 6599  Fax (02) 8263 6561  TTY (02) 9211 3776 (Hearing/Speech impaired)  E:info 45698  F:info 45561

Appendix 4

Report No.53 2003–04  
The Implementation of CrimTrac  
117
Our Ref: 04/003350
Your Ref: 2003/135

Mr David Crossley
Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Mr Crossley,

Comments on Proposed Audit Report – The Implementation of CrimTrac

Thank you for the opportunity to peruse and comment on your proposed audit report following the performance audit into the Implementation of CrimTrac.

Victoria Police concur with all the Recommendations as stated in the report and in the context in which they are made.

The specific concerns expressed by Victoria Police during this Audit relating to the role of the Commonwealth in CrimTrac and the apparent understanding of CrimTrac by the Commonwealth should be accommodated with Recommendation 1.

It was further noted that ownership of the systems and data was not clearly established with some of the Jurisdictions. Appropriate implementation of Recommendation 9 as supported in the report should clarify that issue.

The Issues and Opportunities to Improve raised in your report are noted and will be reflected in subsequent Board of Management policy and decisions for the conduct of CrimTrac.

Yours sincerely,

C. Nixon APM
Chief Commissioner
Mr David Crossley  
Executive Director  
Performance Audit Services Group  
Australian National Audit Office  
GPO Box 707  
CANBERRA ACT 2601

Dear Mr Crossley

PERFORMANCE AUDIT: THE IMPLEMENTATION OF CRIMTRAC

I refer to your letter of 8 April 2004 seeking comments on the proposed audit report on The Implementation of CrimTrac.

The Queensland Police Service appreciates the opportunity to provide input to the report, including by completing your earlier survey regarding CrimTrac’s progress on key deliverables.

The report presents a comprehensive, accurate picture of the issue. I have only two minor comments:

1. Page 28, paragraph 2.81 – Queensland will commence the new pricing model for National Criminal History Record Checks on 1 July 2004.

I trust these comments are of assistance.

Yours sincerely

R ATKINSON  
COMMISSIONER
Mr David Crossley
Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Mr Crossley

PERFORMANCE AUDIT: THE IMPLEMENTATION OF CRIMTRAC

Thank you for your letter of 8 April 2004 and the accompanying draft report of the Australian National Audit Office (ANAO). I appreciate the opportunity to comment on the draft report and provide my in-principle support for the draft recommendations.

In reviewing the document, my attention was drawn to paragraph 3.30 in which the ANAO draft report states that:

"...the Police Commissioners do not appear to make decisions regarding the commitment of the jurisdictional resources necessary to make any systems or procedural changes in the jurisdictions."

I am advised that the ANAO survey form did not identify any specific questions of jurisdictions as to the allocation of resources to meet local systems changes as a result of CrimTrac initiatives. Western Australia Police have established a robust framework upon which systems, processes and procedural changes, in response to CrimTrac systems, are implemented.

In further response to this, I feel that this Service can stand upon its record with respect to the implementation of the National Criminal History Record Checking (NCHRC) project and the leadership role it has taken in the Australian Child Sex Offender Register project to name only two.

I would appreciate the Auditor-General considering these comments before finalising the report.

Yours sincerely

B E MATTHEWS
COMMISSIONER OF POLICE

7 May 2004

Mission Statement: "In partnership with the community, create a safer and more secure Western Australia by providing quality police services."
Dear David

SAPOL’s comments on the performance audit relating to the implementation of CrimTrac follow:

NAFIS
SAPOL agrees NAFIS has been a success that it is much more accurate and efficient than its predecessor. CrimTrac have negotiated an excellent support contract and upgrades have been achieved in a timely manner to ensure there is no deterioration of operations as databases increase. Disaster recovery is the only area that has not been finalised to jurisdictional satisfaction - at this time there could be significant downtime in the event of a major hardware disaster as there is no second "hot" site.

Of particular note NAFIS has provided SAPOL with:

- 1089 identifications from 7900 finger and palm searches during the 2002/03 year.
- 347 identifications on unsolved crime from 21627 searches of new and recidivist offenders during the 2002/03 year.
- the ability to search palm impressions from crime scenes.
- the ability to purchase and utilise Livescan fingerprinting technology.

NCIDD
SAPOL, after consultation with Forensic Science South Australia (FSSA) advise that:

- Contrary to the statement at point 8 in the Executive Summary and later implied at point 2.22, NCIDD is not "developed", rather it is in the primary development stage. That significant issues such as an inability to upload bulk data and match groups, how match groups are to be reported and the format for downloading of data have been identified and remain unresolved. That further problems will only be identified once the "system" is "on line".
- LIMS is only being used by some states - FSSA developed and use SACREDD.(refer 2.22)
- Contrary to the claim "In Crimtrac's view, the system has been "delivered" "only an initial format that requires further development has been delivered. (refer 2.23)
- Some degree of inter-jurisdictional DNA profile matching already exists outside NCIDD. (refer 2.19)

ANCOR
The CrimTrac (ANCOR) Project Team has continued to develop the system through consultation with all jurisdictions and representation on a Registrars Board. The board whose chairperson reports to the CrimTrac Board of Management have met on four occasions since October 2003 and assisted in guiding the project through function and architectural design stages towards testing stages.
Although the project development is on track for an implementation date of July 1 2004, this will not be achievable as it is unlikely that legislation will developed and assented to in all jurisdictions.

Recently, concerns have been raised by the Standing Committee of Attorney’s General through APMC regarding aspects of the draft legislation and proposed ANCRO concept model. The issues of concern will need to be resolved prior to progressing legislative development.

The project has remained within budget with jurisdictions agreeing to contribute to additional funding on a 1/3 – 2/3 basis.

NCOS
In relation to Items 2.32 to 2.43 SAPOL agrees that the report is factually correct.

NCHRC
Page 30 notes that Crimtrac have advised that NCHRC have been fully designed, delivered, and deployed - this is not correct as the NEHRC system (EAMES) is currently under development. SAPOL representatives have undertaken significant work on this and have failed to make any sense of the system so far. Information received from some other jurisdictions indicates a reluctance to fully utilise this systems and that fully manual processes are still being employed.

BUSINESS RECOVERY & CONTINUITY PLANS
Concerns are raised that Crimtrac do not have in place a business continuity plan (BCP) and disaster recovery plan (BRP). This lack of planning on their part could leave the jurisdiction in a very vulnerable situation especially once all of the planned systems come to fruition.

GENERAL COMMENTS
The ANAO report recommends a number of initiatives to improve the performance of the CrimTrac Agency.

There are no objections to any of the recommendations, and in essence they make good business sense. The issue for the Jurisdictions and CrimTrac is how to advance all of these without inadvertently shifting the focus from the CrimTrac project priorities.

It may well be a case for CrimTrac to undertake a joint planning workshop to reassess it’s project deliverables and underlying dependencies. From a jurisdictional view from the outside looking in, it would appear that CrimTrac project managers are readily able to sell concepts and visions for completed applications (CPRS) but do not seem to appreciate the effort and cost to develop the underlying systems and security capabilities. This apparent mismatch may well have contributed to the lack of progress on CPRS. Also adding to poor performance is the ‘re-inventing’ of project priorities, with ANCRO being one example that has recently caused more redirection of resources.

Yours sincerely

Malcolm A Hyde
COMMISSIONER OF POLICE

May 2004
19 May 2004

Mr David Crossley  
Executive Director  
Performance Audit Services Group  
Australian National Audit Office  
PO Box 707  
CANBERRA ACT 2601

Dear Mr Crossley

PERFORMANCE AUDIT: THE IMPLEMENTATION OF CRIMTRAC

I acknowledge receipt of your report and thank you for the opportunity to comment.

I have found the report to be most beneficial in reminding agencies of the history of CrimTrac and its progress in the journey to where we are today. I am confident that the issues and recommendations that are made in the report will inform the CrimTrac Board in a positive manner. The observations and recommendations also provide a signpost to other areas of activity that might benefit by further examination and I would expect that the Board will advance these in the near future.

Unfortunately, Commissioner McCreadie is absent on leave and I am not able to bring to this response his personal views of your report.

Yours sincerely

J JOHNSTON  
Acting Commissioner of Police
Mr David Crossley  
Executive Director  
Performance Audit Services Group  
Australian National Audit Office  
GPO Box 707  
CANBERRA ACT 2601  

Dear Mr Crossley

Thank you for your letter of 8 April 2004, providing me with a copy of the performance audit into the Implementation of CrimTrac, and the opportunity to provide comment.

I have no issues to raise in relation to the report and I concur with its conclusions.

Yours sincerely

Bruce Wernham  
Acting Commissioner of Police

# May 2004
14 May 2004

Mr David Crossley
Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Mr Crossley

PERFORMANCE AUDIT: THE IMPLEMENTATION OF CRIMTRAC

I refer to your letter of 8 April 2004 to Commissioner Keelty regarding the Australian National Audit Office (ANAO) performance audit into the Implementation of CrimTrac. The Commissioner has asked me to respond on his behalf, in my capacity as Chair of the Australian Federal Police (AFP) CrimTrac Advisory Group (CAG).

The AFP supports the ANAO findings and recommendations of the report. The comprehensive audit has clearly identified the key issues for CrimTrac and jurisdictions. We envisage that the recommended use of Memoranda of Understanding or Service Level Agreements to clearly define the roles and responsibilities within agencies will be particularly useful for enhancing working relationships.

Yours sincerely

Peter Jones
Manager
Policy and Strategic Services
(Chair of CAG)

AFP Web site: www.afp.gov.au
## Index

**A**
- Agency Security Advisor, 94
- Attorney-General’s Department, 16, 25-27, 33, 38, 44, 46-47, 57-58, 109, 114-116
- Australasian Police Ministers Council (APMC), 24, 26, 34, 35, 50-51, 57, 59, 61, 67, 75, 111
- Australian Communications-Electronic Security Instruction 33 (ACSI33), 78, 84, 86, 88, 90, 92, 98-99
- Australian National Child Offender Register (ANCOR), 12, 35, 43, 58, 61, 70, 74-75, 79, 108, 110

**B**
- Business Continuity Plan, 14, 18, 81-83, 96, 99, 132-133

**C**
- CrimTrac Board of Management, 16, 25-26, 38-39, 44, 50-52, 55, 57-58, 62, 64-65, 67-68, 70, 72, 82, 109, 111
- CrimTrac Police Reference System (CPRS), 11-12, 29, 31, 34, 36-40, 43-44, 46, 49, 52, 58, 61-62, 69-70, 74, 79, 80, 85, 96, 110
- CrimTrac Programme and Project Management Framework (CPPMF), 14, 17, 62-69, 71-73, 75, 77, 111

**D**
- Disaster Recovery Plan, 14, 18, 81-83, 96, 99
- Disaster Victim Identification Tool, 28, 44
- DNA, 12, 24, 31-34, 44, 57, 94, 110

**E**
- External Agency Management System (EAMS), 41

**F**
- Fingerprint, 27, 29-30

**I**

**J**
- Jurisdiction, 14, 26-27, 31-34, 41, 45, 50, 51, 53, 69, 94, 111
- Jurisdiction – ACT, 11, 26, 80, 100, 114, 125
- Jurisdiction – AFP, 11, 41, 44, 52, 79, 80, 82, 90, 95-97, 110, 113-114, 125
- Jurisdiction – NSW, 26, 32, 34, 39, 44, 74, 94, 117
- Jurisdiction – NT, 26, 124
- Jurisdiction – QLD, 26, 32, 44, 94, 119
- Jurisdiction – SA, 26, 44, 121
- Jurisdiction – TAS, 26, 123
- Jurisdiction – VIC, 26, 32, 39, 44, 94, 118
- Jurisdiction - WA, 26, 120

**M**
- Memorandum / Memoranda of Understanding, 13, 32-33, 41, 53, 57, 70, 79, 93-96, 98, 112
Minimum Nationwide Person Profile (MNPP), 39-40, 61, 63, 67, 70, 74, 75, 95, 110, 112

**N**


National Child Sex Offender System – NCSOS (now ANCOR), 11-12, 25, 29, 34-35, 43, 46, 63, 73-75

National Criminal History Record Checking (NCHRC), 12, 26-27, 29, 40, 42-43, 45-46, 58, 67, 79, 93


National Handgun Buyback Support System (NHBSS), 28, 44, 61, 108

**P**

Police Commissioners Policy Advisory Group (PCPAG), 54-55, 59, 67, 70, 109


Project Coordination Committee (PCC), 24, 62, 64-65, 71-76

Protective Security Manual (PSM), 14, 78, 84-88, 90, 92, 97-99

**S**

Senior Officers Group of the APMC, 26, 50

Strategic Issues Group, 55, 56, 57, 70, 109, 111

**T**

Threat and Risk Assessment (TRA), 79, 85-87

**U**

User Advisory Group, 24, 50, 69, 74, 89
Report No.52 Performance Audit
*Information Technology in the Department of Veterans’ Affairs—Follow-up Audit*

Audit Report No.51 Performance Audit
*HIH Claims Support Scheme—Governance Arrangements*
Department of Treasury

Audit Report No.50 Performance Audit
*Management of Federal Airport Leases*

Audit Report No.49 Business Support Process Audit
*The Use and Management of HRIS in the Australian Public Service*

Audit Report No.48 Performance Audit
*The Australian Taxation Office’s Management and Use of Annual Investment Income Reports*
Australian Taxation Office

Audit Report No.47 Performance Audit
*Developing Air Force’s Combat Aircrew*
Department of Defence

Audit Report No.46 Performance Audit
*Client Service in the Family Court of Australia and the Federal Magistrates Court*

Audit Report No.45 Performance Audit
*Army Individual Readiness Notice Follow-up Audit*
Department of Defence

Audit Report No.44 Performance Audit
*National Aboriginal Health Strategy Delivery of Housing and Infrastructure to Aboriginal and Torres Strait Islander Communities Follow-up Audit*

Audit Report No.43 Performance Audit
*Defence Force Preparedness Management Systems*
Department of Defence

Audit Report No.42 Business Support Process Audit
*Financial Delegations for the Expenditure of Public Monies in FMA Agencies*

Audit Report No.41 Performance Audit
*Management of Repatriation Health Cards*
Department of Veterans’ Affairs

Audit Report No.40 Performance Audit
*Department of Health and Ageing’s Management of the Multipurpose Services Program and the Regional Health Services Program*

Audit Report No.39 Performance Audit
*Integrity of the Electoral Roll—Follow-up Audit*
Australian Electoral Commission
Audit Report No.38 Performance Audit
Corporation Governance in the Australian Broadcasting Corporation—Follow-up Audit

Audit Report No.37 Performance Audit
National Marine Unit
Australian Customs Service

Audit Report No.36 Performance Audit
The Commonwealth’s Administration of the Dairy Industry Adjustment Package
Department of Agriculture, Fisheries and Forestry—Australia
Dairy Adjustment Authority

Audit Report No.35 Business Support Process Audit
Compensation Payments and Debt Relief in Special Circumstances

Audit Report No.34 Performance Audit
The Administration of Major Programs
Australian Greenhouse Office

Audit Report No.33 Performance Audit
The Australian Taxation Office’s Collection and Management of Activity Statement Information

Audit Report No.32 Performance Audit
‘Wedgetail’ Airborne Early Warning and Control Aircraft: Project Management
Department of Defence

Audit Report No.31 Business Support Process Audit
The Senate Order for Department and Agency Contracts
(Financial Year 2002–2003 Compliance)

Audit Report No.30 Performance Audit
Quality Internet Services for Government Clients—Monitoring and Evaluation by Government Agencies

Audit Report No.29 Performance Audit
Governance of the National Health and Medical Research Council
National Health and Medical Research Council
Department of Health and Ageing

Audit Report No.28 Audit Activity Report
Audit Activity Report: July to December 2003
Summary of Outcomes

Audit Report No.27 Performance Audit
Management of Internet Portals at the Department of Family and Community Services

Audit Report No.26 Performance Audit
Supporting Managers—Financial Management in the Health Insurance Commission
Health Insurance Commission

Audit Report No.25 Performance Audit

Audit Report No.24 Performance Audit
Agency Management of Special Accounts
Audit Report No.23 Performance Audit  
*The Australian Taxation Office’s Management of Aggressive Tax Planning*  
Australian Taxation Office

Audit Report No.22 Financial Statement Audit  
*Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2003*  
Summary of Results

Audit Report No.21 Performance Audit  
*Special Employee Entitlements Scheme for Ansett Group Employees (SEESA)*  
Department of Employment and Workplace Relations  
Department of Transport and Regional Services

Audit Report No.20 Performance Audit  
*Aid to East Timor*  
Australian Agency for International Development

Audit Report No.19 Business Support Process Audit  
*Property Management*

Audit Report No.18 Performance Audit  
*The Australian Taxation Office’s Use of AUSTRAC Data Follow-up Audit*  
Australian Taxation Office

Audit Report No.17 Performance Audit  
*AQIS Cost-recovery Systems Follow-up Audit*  
Australian Quarantine and Inspection Service

Audit Report No.16 Performance Audit  
*Administration of Consular Services Follow-up Audit*  
Department of Foreign Affairs and Trade

Audit Report No.15 Performance Audit  
*Administration of Staff Employed Under the Members of Parliament (Staff) Act 1984*  
Department of Finance and Administration

Audit Report No.14 Performance Audit  
*Survey of Fraud Control Arrangements in APS Agencies*

Audit Report No.13 Performance Audit  
*ATSIS Law and Justice Program*  
Aboriginal and Torres Strait Islander Services

Audit Report No.12 Performance Audit  
*The Administration of Telecommunications Grants*  
Department of Communications, Information Technology and the Arts  
Department of Transport and Regional Services

Audit Report No.11 Performance Audit  
*Annual Performance Reporting*

Audit Report No.10 Performance Audit  
*Australian Defence Force Recruiting Contract*  
Department of Defence

Report No.53 2003–04  
The Implementation of CrimTrac
Audit Report No.9 Performance Audit
*Business Continuity Management and Emergency Management in Centrelink*
Centrelink

Audit Report No.8 Performance Audit
*Commonwealth Management of the Great Barrier Reef Follow-up Audit*
The Great Barrier Reef Marine Park Authority

Audit Report No.7 Business Support Process Audit
*Recordkeeping in Large Commonwealth Organisations*

Audit Report No.6 Performance Audit
*APRA’s Prudential Supervision of Superannuation Entities*
Australian Prudential Regulation Authority

Audit Report No.5 Business Support Process Audit
*The Senate Order for Departmental and Agency Contracts (Autumn 2003)*

Audit Report No.4 Performance Audit
*Management of the Extension Option Review—Plasma Fractionation Agreement*
Department of Health and Ageing

Audit Report No.3 Business Support Process Audit
*Management of Risk and Insurance*

Audit Report No.2 Audit Activity
*Audit Activity Report: January to June 2003*
Summary of Outcomes

Audit Report No.1 Performance Audit
*Administration of Three Key Components of the Agriculture—Advancing Australia (AAA) Package*
Department of Agriculture, Fisheries and Forestry—Australia
Centrelink
Australian Taxation Office
## Better Practice Guides

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMODEL Illustrative Financial Statements 2004</td>
<td>May 2004</td>
</tr>
<tr>
<td>Better Practice in Annual Performance Reporting</td>
<td>Apr 2004</td>
</tr>
<tr>
<td>Management of Scientific Research and Development Projects in Commonwealth Agencies</td>
<td>Dec 2003</td>
</tr>
<tr>
<td>Public Sector Governance</td>
<td>July 2003</td>
</tr>
<tr>
<td>Goods and Services Tax (GST) Administration</td>
<td>May 2003</td>
</tr>
<tr>
<td>Managing Parliamentary Workflow</td>
<td>Apr 2003</td>
</tr>
<tr>
<td>Building Capability—A framework for managing learning and development in the APS</td>
<td>Apr 2003</td>
</tr>
<tr>
<td>Internal Budgeting</td>
<td>Feb 2003</td>
</tr>
<tr>
<td>Administration of Grants</td>
<td>May 2002</td>
</tr>
<tr>
<td>Performance Information in Portfolio Budget Statements</td>
<td>May 2002</td>
</tr>
<tr>
<td>Life-Cycle Costing</td>
<td>Dec 2001</td>
</tr>
<tr>
<td>Some Better Practice Principles for Developing Policy Advice</td>
<td>Nov 2001</td>
</tr>
<tr>
<td>Rehabilitation: Managing Return to Work</td>
<td>Jun 2001</td>
</tr>
<tr>
<td>Internet Delivery Decisions</td>
<td>Apr 2001</td>
</tr>
<tr>
<td>Planning for the Workforce of the Future</td>
<td>Mar 2001</td>
</tr>
<tr>
<td>Contract Management</td>
<td>Feb 2001</td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td>Jan 2000</td>
</tr>
<tr>
<td>Building a Better Financial Management Framework</td>
<td>Nov 1999</td>
</tr>
<tr>
<td>Building Better Financial Management Support</td>
<td>Nov 1999</td>
</tr>
<tr>
<td>Managing APS Staff Reductions (in Audit Report No.49 1998–99)</td>
<td>Jun 1999</td>
</tr>
<tr>
<td>Commonwealth Agency Energy Management</td>
<td>Jun 1999</td>
</tr>
<tr>
<td>Cash Management</td>
<td>Mar 1999</td>
</tr>
<tr>
<td>Security and Control for SAP R/3</td>
<td>Oct 1998</td>
</tr>
<tr>
<td>Selecting Suppliers: Managing the Risk</td>
<td>Oct 1998</td>
</tr>
<tr>
<td>New Directions in Internal Audit</td>
<td>Jul 1998</td>
</tr>
</tbody>
</table>
Controlling Performance and Outcomes Dec 1997
Management of Accounts Receivable Dec 1997
Public Sector Travel Dec 1997
Audit Committees Jul 1997
Management of Corporate Sponsorship Apr 1997
Telephone Call Centres Handbook Dec 1996
Paying Accounts Nov 1996
Asset Management Handbook Jun 1996