Commonwealth
OMBUDSMAN

Australian Crime Commission

REVIEW OF COLLECTION, STORAGE AND DISSEMINATION OF INFORMATION

October 2009

Report by the Commonwealth Ombudsman,
Prof. John McMillan, under the *Ombudsman Act 1976*

REPORT NO. 15|2009

Reports by the Ombudsman

Under the *Ombudsman Act 1976* (Cth), the Commonwealth Ombudsman investigates the administrative actions of Australian Government agencies and officers. An investigation can be conducted as a result of a complaint or on the initiative (or own motion) of the Ombudsman.

The *Ombudsman Act 1976* confers five other roles on the Commonwealth Ombudsman—the role of Defence Force Ombudsman, to investigate action arising from the service of a member of the Australian Defence Force; the role of Immigration Ombudsman, to investigate action taken in relation to immigration (including immigration detention); the role of Postal Industry Ombudsman, to investigate complaints against private postal operators; the role of Taxation Ombudsman, to investigate action taken by the Australian Taxation Office; and the role of Law Enforcement Ombudsman, to investigate conduct and practices of the Australian Federal Police (AFP) and its members. There are special procedures applying to complaints about AFP officers contained in the *Australian Federal Police Act 1979*. Complaints about the conduct of AFP officers prior to 2007 are dealt with under the *Complaints (Australian Federal Police) Act 1981* (Cth).

Most complaints to the Ombudsman are resolved without the need for a formal report. The Ombudsman can, however, culminate an investigation by preparing a report that contains the opinions and recommendations of the Ombudsman. A report can be prepared if the Ombudsman is of the opinion that the administrative action under investigation was unlawful, unreasonable, unjust, oppressive, improperly discriminatory, or otherwise wrong or unsupported by the facts; was not properly explained by an agency; or was based on a law that was unreasonable, unjust, oppressive or improperly discriminatory.

A report by the Ombudsman is forwarded to the agency concerned and the responsible minister. If the recommendations in the report are not accepted, the Ombudsman can choose to furnish the report to the Prime Minister or Parliament.

These reports are not always made publicly available. The Ombudsman is subject to statutory secrecy provisions, and for reasons of privacy, confidentiality or privilege it may be inappropriate to publish all or part of a report. Nevertheless, to the extent possible, reports by the Ombudsman are published in full or in an abridged version.

Copies or summaries of the reports are usually made available on the Ombudsman website at www.ombudsman.gov.au. Commencing in 2004, the reports prepared by the Ombudsman (in each of the roles mentioned above) are sequenced into a single annual series of reports.

ISBN 978 0 9806726 8 8

Date of publication: October 2009
Publisher: Commonwealth Ombudsman, Canberra Australia

Requests and enquiries can be directed to the Director Public Affairs, Commonwealth Ombudsman, GPO Box 442, Canberra ACT 2601; email ombudsman@ombudsman.gov.au or phone 1300 362 072 (calls from mobiles charged at mobile phone rates). This report is available on the Commonwealth Ombudsman's website http://www.ombudsman.gov.au.

CONTENTS

EXECUTIVE SUMMARY

In early 2008, an Australian Crime Commission (ACC) senior staff member wrote a note about an official dinner function with a Government Minister. In September 2008, the note was sent to the Minister and was disclosed to the media. These actions raised concerns about the integrity of information gathering and storage at the ACC, particularly as the information related to parliamentarians.

As a consequence, the ACC commissioned investigations into the creation and disclosure of the document and commissioned an independent file management audit. The ACC Chief Executive Officer (CEO) also approached the Ombudsman to conduct a review of the ACC's information holdings to restore government and public confidence in the ACC.

In April 2009, the Ombudsman initiated an investigation into the ACC's collection, storage and dissemination of information. This investigation found no evidence that suggests that the ACC was systematically, or in an organised way, collecting or retaining information that was not related to its serious and organised crime function or was not properly authorised.

We searched for a small sample of current parliamentarians' names in the Australian Criminal Intelligence Database (ACID) and ACC PROMIS databases. This demonstrated that it would be feasible to run limited assurance search audits on these databases. We did not find any records relating to current parliamentarians.

Despite the best efforts of the ACC, the risk of an unauthorised release of information will remain. The ACC should address this risk by establishing clear policy to guide staff behaviour and by fairly and openly censuring breaches of information policy or guidelines.

Current ACC information governance polices are disjointed and several did not cover current operational practices. The ACC's information policy needs to be integrated and simplified.

The policy framework should balance the benefits of information sharing with the need-to-know principle and be supported by effective access-control guidelines and an effective audit regime. Greater consistency in information governance policies would provide clear guidance to staff regarding authorised information management and access. The Ombudsman recommends that the ACC's information policies should make it clear that unauthorised access to information is a serious breach of ACC policy.

The ACC is reviewing the access-control policy for its major document system and developing improved protocols. This needs to be implemented. Access controls and audit measures for other major databases also need to be reviewed. The access controls the ACC implements must be congruent with its stated information policy. The ACC should consider the benefits of a proactive, limited, targeted, information-access audit program.

Our investigation notes the significant efforts the ACC has put into building an integrity culture as an essential and effective information management control measure. Sustained senior management support and adequate resourcing will continue to be required.

We draw to the ACC Executive's attention the impact that the information disclosure incident discussed in this report appears to have had on staff morale and on some ACC staff's perceptions of the management of information and integrity breaches.

Our investigation also highlighted the integrity risks of seconded police officers who are not fully integrated into the ACC culture, and disgruntled employees. The ACC may want to consider how best to manage these risks.

The ACC commented on a draft version of this report prior to its publication and release. The ACC accepted that this report portrayed a realistic picture of the practices and procedures supporting information collection, storage and dissemination in the ACC at the time of the investigation.

The ACC advised that the report's recommendations set out a constructive way to address the identified issues and that it has commenced to address the recommendations. I considered the ACC's comments in finalising this published report.

Recommendations

Arising out of this investigation I make the following recommendations:

Recommendation 1

The ACC should make the development of an overarching information governance policy a high priority. The policy needs to be coherent, take account of existing effective operational practices, be appropriately clear and concrete, balance the benefits of information sharing with the need-to-know principle, provide advice regarding access controls, outline audit functions and provide appropriate definitions and clear advice on sanctions.

Recommendation 2

The ACC should review the duties of the Manager Intelligence Capability and Support Services to ensure sufficient attention can be given to the core responsibilities.

Recommendation 3

The ACC should review the guidance provided to consultant organisations in relation to the use of ACC information.

Recommendation 4

The ACC should develop a definition for 'unauthorised information access' and enforce it. It should be made clear that unauthorised information access is a serious breach of the ACC policy and will be sanctioned as such. The ACC should ensure that staff members are aware of key information access rules and are reminded of their responsibilities.

Recommendation 5

The value of the Random Audit Program should be confirmed by the Executive and the program should be renewed with regular audits and current reports. It may be appropriate to consider devolving audit collection to another level of management and reviewing the collation and reporting task.

Recommendation 6

The ACC Executive should consider improving the ACC's ICT audit and incident reporting systems, as discussed in this report.

PART 1—INTRODUCTION

Background

1.1 The ACC is Australia's national criminal intelligence agency. The ACC works in partnership with other law enforcement agencies to develop a national understanding of serious and organised crime, to provide target information for action by partner agencies and to predict future criminal trends.

1.2 The ACC's CEO, Mr John Lawler APM, approached the Ombudsman to conduct a review of the ACC's information holdings to provide independent assurance that the ACC was not holding improper or unauthorised records on parliamentarians, and was performing its intelligence gathering role in accordance with its statutory function.

1.3 This request followed media reports in September 2008 about a document prepared by an officer of the ACC concerning the then Minister for Home Affairs, the Hon. Bob Debus MP, which was disclosed to the Minister and the media. The ACC, in response to this, commissioned an external quality control report of its file management database from consultants Deloitte Touche Tohmatsu. In October 2008, Deloitte delivered an *Independent observer's report on the ACC search of ADAMA records management system* (Deloitte report). ADAMA is the ACC's principal file management database.

1.4 On 31 March 2009, Mr Lawler commissioned Mr Rob Robinson CNZM to undertake a Governance and Administrative Audit of the ACC (the Robinson Review). The final report of this review was delivered on 30 June 2009 and provided recommendations 'to highlight some issues the ACC needs to resolve to ensure effective implementation of its new Sentinel strategy, and to make good decisions about the allocation of scarce resources'. [1]

1.5 In late April 2009, following further discussion between the Ombudsman and Mr Lawler, the Ombudsman initiated an investigation into the ACC's collection, storage and dissemination of information. On 12 May 2009, the Ombudsman provided an interim report on this investigation to Mr Lawler. The interim report is discussed further in the section on the Deloitte report.

Scope of investigation

1.6 This investigation focused on the policies, practices and controls that the ACC uses to ensure information relevance and security. The investigation was coordinated with the Robinson Review to ensure that any overlap or replication by our investigation was minimised.

1.7 We examined the information governance structure and the management of information in the ACC. This required us to examine the various databases used by the ACC. We examined the policies governing information management, staff integrity and risk management. We also considered the adequacy of stated information access controls and audits.

---

[1] *Report to the Chief Executive Officer of the Australian Crime Commission on the 'Governance and Administrative Audit' of the Australian Crime Commission 2009*. C&M Associates Limited, Wellington, New Zealand, June 2009.

1.8 We did not examine any aspect of the receipt, recording and storage of information received from the national security community.

Investigation methodology

1.9 We assessed the ACC's management of information against the following principles:

- that the ACC collects and manages information in accordance with the requirements of the *Australian Crime Commission Act 2002* (the ACC Act)
- that the ACC has appropriate controls to ensure that ACC intelligence collection, collation, analysis, and dissemination activities flow from decisions made by, and the requirements of, the ACC Board
- that the ACC uses a risk management approach for its databases including ADAMA, ACC PROMIS (the ACC case management database), ACID (the Australian Criminal Intelligence Database) and ALEIN (the Australian Law Enforcement Intelligence Net)
- that the ACC has effective policies and procedures to control, limit and manage information access
- that the ACC has an effective system of information and file management audits
- that the ACC has effective access control exception or incident reporting and access violation investigation and management processes
- that the ACC has developed effective information access training and controls for staff, including induction training, operating procedures and manuals
- that the ACC effectively manages human resources functions, including educating staff about the ACC mission, their role, and the Australian Public Service (APS) Code of Conduct; managing employees who present a risk to ACC information integrity; and taking appropriate disciplinary action for information misuse.

1.10 At the commencement of the review, Ombudsman staff spoke with a member of the staff of the Inspector-General of Intelligence and Security and a member of the Robinson Review. We considered the Deloitte independent observer's report on the ACC's review of ADAMA for any records held on parliamentarians. Between 1 June and 9 July 2009, we interviewed 24 selected ACC managers and staff members at the ACC's Canberra and Sydney offices.

1.11 We reviewed the ACC policy and procedure documents, particularly information, staff integrity and risk-management policies.

1.12 We inspected aspects of the ACC information databases: the ADAMA Records Management System; the ACC PROMIS case management database; ACID; and the ALEIN network. We performed a basic scoping analysis of the ability to perform searches within those databases.

A description of the ACC databases

1.13 The major ACC information management databases are: the ADAMA record management system, the ACC PROMIS case management database, ACID (the criminal intelligence database), and the ALEIN network. ACID centralises national criminal information and intelligence, and facilitates data sharing, analysis and

matching. ALEIN is a secure extranet that provides the gateway to ACID for Law Enforcement Agencies (LEAs) that send, or upload, information to ACID and that can search for and retrieve information. Agencies can also obtain ACC intelligence publications via ALEIN.

1.14 The ACC also manages several other databases: one for national security information, Exam DB, which is the examinations database, and an Oracle structured database.

1.15 The ACC *Intelligence Collection Policy*, which was updated in March 2009, states that the primary repositories for all ACC information and intelligence are ACID and ACC PROMIS.

1.16 The operation of the ACID/ALEIN database and network is one of the ACC's major functions under s 7A of the ACC Act. ACID enables sharing of Highly Protected information with ACC staff and, via the ALEIN network, with client LEAs.

1.17 ACC PROMIS is used by the investigation and special intelligence operations areas of the ACC and functions as an investigation case management tool. ACC PROMIS contains case information which may be incorporated in intelligence reports and uploaded into ACID for dissemination to LEAs.

1.18 ADAMA, a version of the TRIM file management database, was customised for the ACC's use and introduced in early 2007.

1.19 Despite the Intelligence Collection Policy's assertion that ACC PROMIS is a primary repository for ACC information, ACC PROMIS appears to be becoming less important as a database in which to initially record and manage intelligence information before upload to ACID. For example, during our investigation we encountered an investigation for a Determination and a Special Intelligence Operation that had limited the information in PROMIS to case management and case tasking, and instead, relied on ADAMA to manage sensitive case information. We were advised that the Financial Intelligence Assessment Team (FIAT) uses ACC PROMIS for case management and ADAMA for information management, and then uploads the intelligence from ADAMA to ACID.

The ACC staffing arrangements

1.20 The ACC employs the majority of its staff under the *Public Service Act 1999* (Public Service Act*)*. The ACC also employs staff under two other arrangements, both under provisions of the ACC Act.

1.21 Section 48 of the ACC Act allows the CEO to engage 'persons having suitable qualifications and experience as consultants to, or to perform services for, the ACC'. The ACC has used this method to engage private sector financial institution employees as ACC consultants to work on the Financial Crimes Determination.

1.22 Section 49 provides that the ACC 'shall be assisted in the performance of its functions' by members of the Australian Federal Police (AFP), employees of authorities of the Commonwealth and persons whose services are made available to the ACC from a state government agency, such as a member of a state police force (seconded officers).

1.23 Section 4 of the ACC Act defines all of these classes of employees as members of the staff of the ACC. All members of staff are subject to the s 51 secrecy provisions (discussed in paragraph 2.28 of this report). Current ACC policies require all staff to adhere to the APS Code of Conduct. However, staff employed under s 48 and s 49 cannot be sanctioned under the Public Service Act for a breach of the APS Code of Conduct. We examine this further in a later section of the report.

PART 2—INVESTIGATION

The environment

2.1 The ACC is undergoing significant review and redirection. A partial organisational restructure occurred in mid 2008. Mr Lawler commenced as the new CEO in March 2009. The Attorney-General's Department is developing an Organised Crime Strategic Framework which is likely to suggest changes to the Government's approach to organised crime and which may impact upon the ACC's activities.

2.2 There were two reviews of ACC governance occurring in 2009: the Robinson Review into the ACC's higher-level governance and administrative arrangements; and this investigation.

2.3 The Robinson Review focused on ACC top-level governance, resources, intelligence practice, performance and relationship management. The review report seeks to position the ACC within the developing Commonwealth Organised Crime Strategic Framework and to enable the ACC to operate effectively within its financial resources.

2.4 The ACC is developing a new operating model, the 'Sentinel Strategy', focusing the agency's resources on targeting higher value serious and organised crime.

2.5 In 2008, the ACC commenced a process of enhancing its integrity culture. This included updating professional standards policies and processes, developing and rolling out management training and ethics, and integrity training.

2.6 Several major governance policies are in draft, including the *Workplace Behaviour Policy, Complaints Policy and Standard Operating Procedure*, a new *Information Management Policy*, the *Clear Desk Policy* and the *Information Technology Security Policy*.

2.7 We are advised that these draft policies are being considered by General Managers. For this reason, in some instances we have considered and commented on both published and late-stage draft policies where together they provide a picture of how the ACC Executive and management are addressing relevant issues.

The creation of ADAMA record—08/46107

2.8 This investigation arose from the creation and disclosure of an ACC document, ADAMA record 08/46107.

2.9 Mr X, an ACC General Manager, created ADAMA document 08/46107 on 10 April 2008. We examined a copy of the document. Mr X made notes about an official dinner in Alice Springs on 9 April 2008 with the then Minister for Home Affairs, the Hon. Bob Debus MP, his wife, his advisers, members of the Australian Federal Police and another ACC officer, Mr Y. The notes summarised the evening and included specific comments on the Minister's habits, the Minister's political affiliations, his interest in police corruption, and the Minister's views on the ACC. The notes concluded with a salutation 'Rgds [Mr X]'.

2.10 At 12.05 pm on 10 April 2008, Mr X forwarded to the ACC Executive Directors an email which included a copy of notes by Mr Y on an official briefing given to the Minister on 9 April 2008. Mr Y's notes were a summary of the discussion on police

and ACC issues related to the Northern Territory Intervention, and on the Minister's and his advisers' comments on those matters.

2.11 Mr X forwarded the ADAMA document 08/46107 to ACC Executive Director Mr Z at 12.06 pm. He asked Mr Z not to forward his notes, as he intended to chat with Mr Z about them. Mr X noted that he had jotted them down as 'it might assist the CEO in future meetings/briefings'.

2.12 An unknown person mailed a hard copy of ADAMA 08/46107 to Minister Debus's Parliament House office, where it was received on 16 September 2008. The Minister advised the then ACC CEO, Mr Alastair Milroy.

The investigation of access to ADAMA 08/46107

2.13 On 17 September 2008, the Minister passed the document to Mr Milroy. The ACC then commenced an investigation. We have examined the investigations into the disclosure of ADAMA 08/46107 in some detail as they provide a lens through which we were able to examine the systemic issues that became apparent.

2.14 Mr X responded to written questions put to him by Mr Milroy on 18 September 2008. He stated that the document 'was first and foremost personal and private notes for myself' and 'a further purpose of the document was (if required), for my personal notes to form the basis of a briefing to the Senior Executive of the ACC about the visit of Minister Debus and the dinner. I acknowledge that some of the comments/notes were completely irrelevant and benign but were personal notes'. He described them as 'a brain dump' and that as a former police officer he was accustomed to making prolific notes. Mr X wrote 'at the time of making the notes in relation to the Minister, it was never intended to share those thoughts or observations with anyone'.

2.15 Mr X stated in his written response to Mr Milroy that he had 'compiled this document in naivety about the political process', that he had sought to better inform the ACC Executive about the Minister's interests and the discussions. Mr X concluded by offering his regret and apologies to the Minister and his wife, and to Mr Milroy.

2.16 The ACC also commissioned two external investigators, Mr Boris Budak and Mr Bill Stoll, to review aspects of the matter.

The Budak review

2.17 Mr Budak considered whether the content of Mr X's document was appropriate and if he may have breached the APS Code of Conduct. On 8 October 2008, Mr Budak reported that the document was carelessly prepared and stored. He reported that there was evidence that Mr X may have breached the Code of Conduct, but that this was for a decision maker to determine. The ACC advised our investigation that Mr X was sanctioned for a breach of the Code of Conduct.

The Stoll investigation

2.18 The ACC advised that it engaged Mr Bill Stoll to investigate the access to ADAMA 08/46107 and its disclosure to the Minister.

2.19 Mr Milroy had asked Mr X to respond to a set of written questions relating to the creation and dissemination of the ADAMA document. Mr X stated that he believed that he had locked down document access to himself only. Mr Stoll's

investigation report advised that the document was left with the ADAMA 'default setting' of open, meaning it could be viewed by all staff with ADAMA access.

2.20 The default setting is for ADAMA documents to be saved as open access, so that the document content and document metadata can be accessed by any member of staff of the ACC. Document metadata includes, for example, the title, creation date, and author, and is that information attached to the document that enables a document to be searched for and retrieved.

2.21 The creator of the document must consciously choose to impose access controls if they wish to lock down the contents of their document from view. They can also choose to restrict the metadata from view, or restrict the metadata so that it can only be viewed by selected people or access groups.

2.22 Mr Stoll's investigation considered the ADAMA access logs and determined that five ACC employees had accessed the document on particular dates and times, before the Minister reported the matter to the CEO.

- Ms A, an ACC staff member, accessed Document 08/46107. She stated she did not print it and she sometimes searched ADAMA to see what was happening in the area in which she and Mr X worked. She stated she did not have Mr X's authority to view the document and believed that she was allowed to access an unlocked document.
- Mr B, a police officer seconded to the ACC, read the document while looking for an 'order of merit' list for potential employment at the ACC. He stated he did not print or disseminate it. Mr X's notes indicated that on another occasion Mr B had told him a copy of a personal document by Mr X had been 'floating' around the section of the ACC office where Mr B worked. Mr X believed that someone at that section of the ACC office had been searching and copying his personal ADAMA documents.
- Mr C, an ACC staff member, accessed the document and admitted to printing it. He said he was researching a complaint he had made to the Integrity Commissioner and he was looking for a report/response from Mr X in response to a Freedom of Information request he had submitted.
- Mr D, an ACC staff member, admitted accessing the document while looking for background information for a work-related task. He showed the document to a colleague on his computer screen. Both denied printing or discussing the document with anyone else.

2.23 Two of the staff who accessed the document, Mr B and Mr C, stated reasons for doing so that appear, on their face, to be unrelated to the performance of their duties. Ms A said she was browsing to see 'what was happening' in her work area. Ms A, Mr B and Mr C stated that the ACC position was that information in ADAMA was for open access, unless a document was locked down.

2.24 Mr Stoll was unable to conclusively say who had sent the copy of ADAMA 08/46107 to the Minister's office. The ACC Executive, after consideration, decided not to pursue the issues of Mr B's or Mr C's accessing of ADAMA 08/46107. Mr B returned to the state police and we understand that Mr C is on personal leave.

2.25 The ACC referred Mr Stoll's report and the matter to the Integrity Commissioner as a possible corruption matter.

ACC information policy and legislation

The current information policy

2.26 The ACC is an information and intelligence agency. Subsection 12(6) of the ACC Act commits the ACC to an information-sharing approach. It states:

> Where the ACC has obtained particular information or intelligence in the course of performing one or more of its functions, nothing in this Act shall be taken to prevent the ACC from making use of the information or intelligence in the performance of any of its other functions.

2.27 The ACC Establishment Bill 2002, Revised Explanatory Memorandum, at items 42 to 49 states:

> Subsection 12(6) is an important provision that recognises the continuum between intelligence, intelligence operations and investigations. It is essential that the use of information that is relevant to one function is not artificially restricted by unnecessary compartmentalisation of the functions of the ACC.

2.28 The ACC Act contains a secrecy provision, s 51, which applies to all ACC staff, examiners, the Board and the CEO. Section 51 states:

> A person to whom this section applies who, either directly or indirectly, except for the purposes of a relevant Act or otherwise in connection with the performance of his or her duties under a relevant Act, and either while he or she is or after he or she ceases to be a person to whom this section applies:
>
> (a) makes a record of any information; or
> (b) divulges or communicates to any person any information;
>
> being information acquired by him or her by reason of, or in the course of, the performance of his or her duties under this Act, is guilty of an offence punishable on summary conviction by a fine not exceeding 50 penalty units or imprisonment for a period not exceeding 1 year, or both.

2.29 An intelligence organisation, in building an information system, must take a risk management perspective and strike a balance between information sharing and imposing restrictions to prevent unauthorised information disclosure. This is the balance between the need to share information and the requirement to impose a need-to-know policy. It is easier to see and measure the risks of unauthorised disclosure and it is harder to measure and balance the risks of not sharing information.[2] The ACC Executive Director, Organisational Services told our investigators that the ACC needs to maintain the balance towards a more open system. We were also advised that the ACC had made some changes to its ADAMA access control, for example limiting access for some documents to relevant functional areas, and that the ACC was reviewing ADAMA access control guidelines.

2.30 The management view appears to be that the organisation has adopted a need-to-share philosophy, yet pockets within the organisation still adopt the need-to-know approach. Adherence by some officers to a need-to-know principle was demonstrated in a recent article in *The Australian* newspaper:

---

2 *Mobilizing information to prevent terrorism; Accelerated development of a trusted information sharing environment,* third report of Markle Foundation Taskforce. The Markle Foundation, New York City, July 2006, page 8.

> One source told *The Australian* the ACC had no knowledge of the officer's alleged misconduct when he was hired in 2004. Another source played down concerns the officer would have enjoyed widespread access to high-level intelligence, saying the ACC operated on a strict need-to-know basis. [3]

2.31 We return to this issue later in this report and specifically in Recommendation 4.

2.32 In February 2009, the ACC Executive performed a risk assessment process with KPMG, which it reported as an *ACC Risk Scorecard*. The scorecard demonstrated that ACC top management recognised the complexity of information management in the ACC and the need for a 'strategic' and 'an organisationally consistent approach to information management'. This scorecard noted that policy redevelopment was occurring but that many policies remained in draft.

2.33 The *ACC Fraud Control Plan 2009–2011* lists three of its six fraud risks as versions of compromise of data integrity, or leaks, and states:

> The most cost effective means for preventing, detecting and deterring fraud in any organisation is the establishment and reinforcement of a sound ethical culture with a high level of staff awareness of the risk of fraud and the impact that fraud would have on its sustainability.

2.34 The organisation's culture—the shared standards, values and mores of staff—is integral to maintaining information security. In response to leaks such as the one examined in this report, the ACC responded in 2008 by taking steps to strengthen its culture of integrity. Recent actions include an increased effort in ethics training (emphasising the APS Code of Conduct), increased management and multi-disciplinary education, an improved and standardised induction for all staff, increased integrity and operations audits by the Professional Standards area, and a re-drafting of the relevant professional standards, workplace behaviour and complaints policies.

2.35 The other key organisational control element is the presence of clear, well disseminated, top management supported and documented policies and messages that direct and control the collection and management of information.

2.36 At the time of this investigation, the relevant ACC policies and instructions on accessing ACC information were not coherent: the guidance was scattered through numerous policies and directions, and several information-related policies were not up-to-date. For example, at the commencement of our investigation we were supplied with the *Information Management Plan 2004 to 2007*. This plan is descriptive and not prescriptive, the language is general and overall it represented an imprecise guideline.

2.37 Until recently there was a clear direction from top management that ACC information was to be on open access to staff. An *All Staff Message from the CEO*, number 39/03 dated 19 August 2003, encouraged information sharing and uploading of information from ACC PROMIS to ACID. The CEO's message advised that sensitive material, including 'where official corruption may be involved' or 'developments that are likely to attract media or ministerial attention', was to be marked in ACC PROMIS as 'Management Significant Entries' so as to bring such matters to senior management's attention.

---

[3] *Queensland corruption; Crime body tainted by rogue cop,* The Australian, 30 July 2009.

2.38 The clearest policy direction at the time of access to ADAMA 08/46107 was provided by the ACC IT Security Policy, dated March 2005. This policy set the requirement for the secure operation of information and communication resources within the ACC and applied to all staff. The policy predated the ACC's commencement of ADAMA in 2007.

2.39 The IT Security Policy was approved by then CEO Mr Milroy and was current in June 2009 at the commencement of our investigation. It has subsequently been withdrawn for redrafting.

2.40 The IT Security Policy appears to be the one major policy that clearly set out the requirements for the secure operation of information and communication resources and which applied to all staff. This policy preferred the need-to-know principle and did not emphasise a need-to-share approach. As such, it conflicted with the need-to-share message which was reinforced when ADAMA was launched. This appears to represent a conflict in the organisation's messages about information security.

2.41 The policy stated at paragraph 4.2: 'staff may only access the ACC ICT Systems, functions and data that they have been authorised to use, and may only do so for legitimate ACC business associated with the performance of the duties of the position they occupy'. This section draws upon the secrecy provision in s 51 of the ACC Act. The policy also stated at section 13.1, that access was granted on the basis of the 'requestor's need-to-know'.

2.42 The policy also had a section on information misuse. Section 13.3 defined misuse as just cause for sanctions. Information misuse included: 'accessing ICT resources without proper authorisation' and 'taking advantage of another staff member's negligence to gain access to the ACC's ICT resources for which they have not been authorised'.

2.43 The IT Security Policy provided guidelines for information access control which were appropriate to sanctioning the access that occurred in respect of ADAMA 08/46107. It is arguable that both Mr B in seeking 'correspondence "pertaining to the order of merit" list for potential employment at the ACC', and Mr C in 'looking for a report/response from [Mr X] in relation to an FOI request he had submitted', were not performing their duties when conducting these searches. Mr C by printing off a copy may also be considered to be 'making a record' and he admitted that he discussed the document with other members of the ACC; as such he may have been in breach of the s 51 secrecy provision of the ACC Act.

2.44 An all staff message from the CEO, dated 22 September 2008 and titled *Information Management* was released soon after the ACC was notified of the disclosure of Mr X's ADAMA document. The CEO's message stated:

> To support the ACC's intelligence function, ADAMA access controls have been configured to support the 'Need to Share' principle. This allows staff full access to the information they need in ADAMA to undertake their role. Staff are reminded, however, that they must not actively seek information in ADAMA that they have no business need to access. Auditing of access to information in ADAMA is and will continue to be carried out.

2.45 In our view, the ACC's information policy has not to date presented a coherent message. There was no policy framework that combined and described for staff the appropriate balance between the need-to-know policy and the benefits of information sharing and which unambiguously guided staff behaviour. However, there

was no ambiguity about the ACC policy which prohibited the release of ACC information to the media without authorisation.

The draft information management policy and ACC information charter

2.46 An early draft of an *Information Management Policy* and a draft of an *ACC Information Charter* were available to our investigation.

2.47 The draft Information Management Policy lacks specificity. It fails to address squarely the tension between the benefits of information sharing with the need-to-know principle. The draft policy is aided by a draft sub-document, the draft ACC Information Charter, which serves to split up the guidance information yet again.

2.48 The draft Information Charter is general but it does state on the first page: 'central to making effective use of our information is information sharing: within the ACC and with our customers'; and it later states; 'ACC management shall maintain an organisational culture in which information sharing is a core organisational activity'. However, the draft Charter shows little hierarchy of the importance of information management rules. It does address the need-to-know principle in a lower dot point: 'ACC staff shall only access information which is reasonably needed to perform their duties'.

The need-to-know principle and current operational access control measures in ADAMA

2.49 We interviewed operational and analytical staff who emphasised the importance in their roles of the need-to-know principle to protect mission critical operational information. They demonstrated this with current examples in their work area where, in ADAMA, document text information and spreadsheets were locked to small functional teams. Metadata tended to be left unlocked to allow wider ACC searching and access. Extremely sensitive information (such as discovered corruption) was tightly access controlled. One staff member emphasised the importance of clear document titles to assist metadata searches. Team Leaders, Heads and Assistant Heads of Determinations managed requests for access to information collected by their teams.

2.50 Intelligence is sanitised and uploaded to ACID towards the end of operations or investigations when it is judged safe to do so. Some particularly sensitive information is not uploaded to ACID, both to protect the information integrity and to protect the important relationship with the ACC information provider.

2.51 No current ACC information policy adequately captures, supports or guides these operational practices.

Recommendation 1

The ACC should make the development of an overarching information governance policy a high priority. The policy needs to be coherent, take account of existing effective operational practices, be appropriately clear and concrete, balance the benefits of information sharing with the need-to-know principle, provide advice regarding access controls, outline audit functions and provide appropriate definitions and clear advice on sanctions.

Risk management

2.52 The ACC operates in a complex environment with many potential risks. Our investigation requested a copy of the ACC risk register and was advised that the organisation did not have one. We examined the most recent available *Bi-Annual Risk and Action Reports,* which were completed by business areas and are dated January 2008.

2.53 There appeared to be a fragmented approach to prioritising and highlighting major organisational risks for attention by the Executive. Until recently, responsibility for risk management was assigned to a range of managers—the Manager for Strategic Planning Risk and Governance, each Executive Director, including the Executive Director Organisational Services, and the CEO. Risk management was also devolved to business areas, which produced detailed plans and strategies to recognise and mitigate risks. The Audit Committee was charged with providing advice to the CEO on the management of risk and the adequacy of ACC internal controls.

2.54 The lack of strategic risk oversight was considered in February 2009, when KPMG conducted and delivered a *Risk Scorecard Report*. This scorecard was a frank assessment for the Executive of the major risks facing the ACC.

2.55 We were advised that the ACC has begun to redesign its risk management and risk information systems. There is a *Risk Management Policy* (dated March 2008), and a new *Risk Management Strategy 2009–11*. The Senior Executive Risk Management Sub-committee was formed in 2009 and is defining its role. Risk management is being driven by the Executive Director, Programs. One task appears to be to define the roles and reporting pathways for the Senior Executive Risk Management Sub-committee and the Audit Committee.

2.56 The ACC has recognised a gap in reporting to the Executive about risk incidents and has begun to develop an Incident Reporting pathway and system.

The Deloitte independent observer's report

2.57 Following the disclosure of ADAMA 08/46107, the ACC engaged Deloitte as consultants to observe and verify a search of the ADAMA record management system for references to current parliamentarians. The Deloitte review of ADAMA was limited to metadata and title fields and 'these procedures are substantially less in scope than a reasonable assurance audit'. The results of the review were that there were no inappropriate records relating to current parliamentarians being held in the ADAMA system.

2.58 The Ombudsman provided an interim report of this investigation dated 12 May 2009 to the ACC CEO. In that report, the Ombudsman concluded that after examining all the documents provided, it was his view that the Deloitte review was appropriately conducted and its methodology sound. Importantly, the Ombudsman advised that if Ombudsman staff were to conduct a similar review, the same limitations would apply to any findings.

2.59 During our investigation, we sought further clarification from Deloitte as to why a metadata and title search and not an ADAMA document text (or content) search had been done. Deloitte advised that ADAMA had the capability to perform a text search but it was not done for several reasons. A text search would be an enormous task, it would be slow, it would be costly, it would raise significant security

issues as a consequence of the search, and it would interfere with the normal operation of ADAMA and the ACC.

2.60 To verify these claims we tested the ability to search ADAMA with the assistance of an ACC ADAMA administrator. We did a trial document text or content search of the database through the ADAMA interface and also through the 'back-end' of TRIM. The content searches were slow and some did not complete within a 20-minute time frame. We were advised that content searches could become unstable and the search would not infrequently lock up and cease. In contrast, metadata searches were quick and effective. We confirmed our conclusion that, given current available ADAMA search facilities, a search as conducted by Deloitte is the most effective way to review ADAMA holdings as a whole.

Searching other ACC databases

ACID/ALEIN

2.61 The ACID database is extensive and can be searched by data entities such as a person's name, address or occupation. We searched a small sample of current parliamentarians' names to test the ability to run assurance checks on this database. The searches did produce some limited records related to previous parliamentarians. These records appeared to have been created for proper and reasonable purposes.

2.62 Our testing demonstrated that it would be feasible to run assurance audits on the ACID database. Given the size of the database, selected or random samples could be run. An exhaustive search of the ACID database would have exceeded our investigation's time and resources.

2.63 A recent ACC commissioned review of ACID/ALEIN was conducted by Deloitte and reported in April 2009. The review produced the *Deloitte ACID review risk register*. The risk register detailed multiple information security and handling risks related to ACID/ALEIN. For example, the review found that Memorandums of Understanding (MOUs) governing ACID users in client LEAs were outdated and some were lacking current signatories. Documents released from ACID did not retain their appropriate *Protective Security Manual* security classification.

2.64 The ACC has responded to, and completed an assessment of the Deloitte Review incorporating the *Australian Government Information and Communications Technology Security Manual* and has prioritised the top nine risks. The ACC is developing fresh MOUs, is drafting a new *ACID/ALEIN System User Standard Operating Procedure* and has drafted a *User Undertaking and Declaration*. The proposed User Undertaking and Declaration requires users to acknowledge that access to ACID is for legitimate business purposes only and that users have an obligation to report incidents and to keep a record or log of their access to ACID, including dates and reasons which the ACC may require for audit purposes.

2.65 We were also advised that the ACC has allocated $27,000 to commence intrusion testing of ACID/ALEIN. The ACID developments outlined above appear to be appropriate and necessary responses that should be finalised as soon as possible.

2.66 The Ombudsman notes that the Manager, Intelligence Capability and Support Services (IC&S), has also assumed responsibility as business manager for ACID/ ALEIN. Given the challenges facing ACID/ALEIN, the dual roles may overload that position.

Recommendation 2

The ACC should review the duties of the Manager Intelligence Capability and Support Services to ensure sufficient attention can be given to the core responsibilities**.**

ACC PROMIS

2.67 The ACC PROMIS database can be searched by data entities such as a person's name and address. In ACC PROMIS we also searched a small sample of current parliamentarians' names to test the ability to run assurance checks on this database. We searched by person entity and *'Ntext',* which searches numerous text fields. We did not find any records relating to current parliamentarians.

2.68 Our limited testing demonstrated that it would be feasible to run assurance audits on the ACC PROMIS database. Given the size of the database, selected or random samples could be run. A thorough search of the ACC PROMIS database would have exceeded our investigation's time and resources.

The collection of information

2.69 Section 7A of the ACC Act authorises the ACC to collect criminal information, to maintain a national database of that information and intelligence (ACID), and with Board authorisation to undertake intelligence operations and investigations. The Australian Crime Commission Establishment Bill 2002, Revised Explanatory Memorandum, explains:

> Paragraph 7A (a) provides a general intelligence function designed to give the ACC the widest possible power to collect, correlate, analyse and disseminate criminal information and intelligence with prior approval by the Board. This function enables the ACC to pursue lines of enquiry (including conducting probes), receive information and assess the value of that information so long as it is within priorities endorsed by the Board.
>
> The determination of national criminal intelligence priorities will form the basis for the action undertaken by law enforcement authorities across Australia, whether it is the ACC or police forces from the Commonwealth, States and Territories. This will provide an enhanced and coordinated national law enforcement capacity, which will set national law enforcement priorities.

2.70 Sections 7A(b) and 7A(c) of the ACC Act provide for the Board to authorise intelligence operations and investigations.

2.71 We examined the documentation for Board approval of the ACC *National Criminal Intelligence Priorities* (NCIPs) 2009–10. We examined Board approval and completed documentation and instruments for the *Australian Crime Commission Special Investigation and Determination (Financial Crimes) 2008* and Amendment No. 1 of 2009 which authorise a special investigation. We also examined Board approval and completed documentation for the *Australian Crime Commission Special Investigation Authorisation and Determination (High Risk Crime Groups No 2) 2009*.

2.72 The Board authorises the NCIPs, which guide the ACC's and Australian LEA's collection of information. The process for authorising the ACC's collection of information appears to be soundly managed. All ACC staff we interviewed displayed

a clear understanding of the ACC's function to investigate and collect intelligence on serious and organised crime.

2.73 We interviewed the ACC Head of Determination, and an investigator from a Special Intelligence Operation. In relation to the Financial Crimes Determination, we interviewed the Manager of the FIAT. We interviewed staff and examined documents authorising the collection of information for a fraud detection project, the Suspected Financial Crimes Intelligence Network (SFCIN).

2.74 The projects under the Financial Crimes Determination are innovative and seek to position the ACC to provide intelligence to interrupt criminal activity and to target the financial resources of organised crime groups. The SFCIN is an ACC flagship project established to enable collection of suspected financial crimes data from private sector financial, banking, telecommunications and insurance organisations. Data is obtained from these organisations under a s 29 notice signed by an ACC examiner to authorise that collection. The collected data is 'washed' against ACID data and analysed for matches to create intelligence on serious or organised crime.

2.75 The ACC advised that it invests time in building trust and communication with the staff in private sector financial institutions who assist the ACC by providing information to enable the work of the SFCIN. These relationships are formalised by using s 48 Consultancy Agreements. Once signed, these agreements make private sector (security cleared) staff a 'member of the staff of the ACC' under s 4 of the ACC Act and subject to the s 51 secrecy provision.

2.76 As there are statutory limitations which prevent the ACC from passing information to the private sector, the SFCIN provides only general information to the private sector agencies which assists them to harden their processes against criminal activity.

2.77 We have a concern with the ACC document *SFCIN—Frequently Asked Questions* (FAQs), which provides advice to consultant private sector organisations. The document advises consultants that they may not use data or lists obtained through consultation with the ACC—'no information provided by the ACC can be placed on, for instance, a "suspect" or "black list" [within their organisation] however, consultants can make further enquiries within their own systems to identify any further information which would assist them in combating fraudulent activities i.e. a "red flag" to further investigate'.

2.78 The ACC advised us that they take care to ensure that the consultant companies do not develop black lists or black flags. The advice in the FAQs conflicts with the advice the ACC provided to our investigation. The FAQ appears to allow a consultant to use ACC-provided information or lists as a starting point or 'red flag' for further private sector organisation investigation. This may not be appropriate.

2.79 The SFCIN initiative is innovative and it leverages the ACC's ability to collect information and expands its reach into the private sector. The ACC must continue to take care with the governance of this information channel, in particular to maintain the lawfulness of the information collection approaches. On this basis, it would be reasonable for the ACC to review the Consultancy Agreements and General Conditions for Consultancy Services.

Recommendation 3

The ACC should review the guidance provided to consultant organisations in relation to the use of ACC information.

Dissemination of information

2.80 The *Disseminations Policy* is clear and current. There is also a *Disseminations Standard Operating Procedure* (SOP) currently in draft.

2.81 Dissemination of intelligence is authorised by the ACC Act. The Board authorises dissemination under s 7C(1)(g) and the CEO or delegate authorises dissemination under s 59(7)–(11). For example, completed Strategic Criminal Intelligence Assessments are provided to the Board before uploading to ACID/ ALEIN for dissemination.

2.82 The primary mode of dissemination of ACC intelligence is via the ACID/ ALEIN network. The ACC has completed a risk analysis for ACID/ALEIN which will guide future needed improvements in information security. Areas for improvement include the updating of ACID/ALEIN client user MOUs, and addressing a concern that documents printed from ACID may not have retained their original security classification. The ACC has also indentified that ACID/ALEIN users may be able to access documents that exceed their, or their systems, level of security clearance.

2.83 The intelligence derived by SFCIN when disseminated from ACID contains the caveat that the intelligence may involve persons who have been the victim of identity fraud. The aim is to reinforce that some identities may not be suspected criminals and that caution should be employed when using the intelligence from SFCIN.

Access controls

2.84 As previously discussed, the default setting for ADAMA documents is for open access to text and metadata information. The ACC Acting Chief Information Officer (CIO) advised that some access control groups currently exist. For example, during our investigation we had to request that access be granted to some corporate and compliance documents which were locked down.

2.85 The ACC has commenced a project to examine access control and to make recommendations for change. We understand that this Access Control List Modification Project is due to report soon and may recommend locking down ADAMA documents to control groups that would represent functional groups or teams reporting to, for example, a General Manager.

2.86 During our investigation we were advised of some other examples of unauthorised information leaks of ACC documents. During interviews we were informed of operational areas that, on the basis of information sensitivity and a need-to-know requirement, have locked down ADAMA document access to their team(s) or to particular people. We were also advised that, where possible, it was important to leave metadata access open to enable document searches to comply with, for example, subpoenas for all documents relating to a person, FOI requests or business purposes.

2.87 We understand that problems have occurred with the migration of pre-ADAMA information to ADAMA, including previously locked documents becoming open access documents. We also understand that there were examples where a previously locked document was copied for legitimate business purposes and the copy then defaulted to open access.

2.88 The Ombudsman notes the complexity of access controls and supports the development of appropriate locking of text data and the development of clear guidelines for staff. It would seem appropriate that business or operational information owners have adequate authority to determine the necessary mix of securing and sharing data in their areas—based upon clear guidelines and a balancing of risks.

Defining and censuring information access breaches

2.89 In the earlier section titled *ACC information policy and legislation*, we outlined the goal for the ACC to establish an information policy that explicitly balances the need to share with what the ACC determines are the necessary need-to-know limitations, and the consequent operational access controls. This is to provide the necessary clear guidance for staff and to organise and structure the other related and subordinate ACC policies.

2.90 The Ombudsman acknowledges that it is for the ACC to determine the appropriate balance between the need to share and the need to know. The ACC, after establishing and having disseminated this policy setting to its staff, will be in a better position to set clear boundaries for staff information access rules and penalties for breaches.

2.91 In the case of ADAMA 08/46107, Mr Stoll's investigation and the ADAMA audit logs were able to demonstrate that two, and possibly three, staff were browsing corporate records for their own purposes. The ACC was not able to prove who disclosed the information.

2.92 If unauthorised information access was considered a breach of ACC rules and policy, the ACC would not need to take the further and more difficult step of proving who leaked the information. The IT Security Policy provided for this lower threshold and is now being redrafted. The ACC has the capability via its audit logs to determine who accesses ADAMA information. It may be useful to augment this ability with audit logs of search terms. Such a log could retrospectively demonstrate any aberrant searches or unauthorised 'fishing expeditions'.

2.93 An appropriate definition of 'unauthorised information access' would grade inappropriate information access as a serious breach of ACC policy. The AFP includes such a definition within its conduct system.[4] For the AFP, 'Information Access [unauthorised]' is serious misconduct which can be sanctioned by dismissal.

2.94 To protect staff from the inadvertent breach of such a rule, the ACC would need to ensure that staff were made fully aware of the policy.

2.95 One way to inform staff of the policy, and the expected behaviour, could be to employ computer screen warnings—'splash screens'. For example, the AFP employs

[4] Australian Federal Police Categories of Conduct Determination 2006, *Australian Federal Police Act 1979.*

a splash screen on computer login that reminds staff of the rules about browsing and unauthorised access to information.

2.96 The IT Security Policy stated that the ACC uses a splash screen, but there was no splash screen in use in the ADAMA or Citrix operating environment during our investigation. We enquired and were advised that with the move from a Novell to a Citrix environment, concurrent with the introduction of ADAMA, those screens had ceased. We note that splash screens have recently been introduced into ACID and ALEIN and that there is an intention to update them as guidelines and SOPs are approved.

2.97 Making private sector employee members of the staff of the ACC is not without risk. The ACC needs to be able to manage these staff members. The Ombudsman notes that, due to their employment arrangements, any breaches of guidelines by such staff would be outside the APS Code of Conduct and would need to be addressed as breaches of s 51. This could involve criminal proceedings and, potentially, be conducted in public. This is made clear in the ACC Consultancy Agreements.

Recommendation 4

The ACC should develop a definition for 'unauthorised information access' and enforce it. It should be made clear that unauthorised information access is a serious breach of the ACC policy and will be sanctioned as such. The ACC should ensure that staff members are aware of key information access rules and are reminded of their responsibilities.

Random audits and operational audits

ICT random audits

2.98 Numerous policies and interviewees mentioned that random audits of ACC information holdings occurred. Recently employed and managerial staff advised that random IT audits occurred. We confirmed with the Acting CIO, the Information Technology Security Adviser (ITSA) and the Manager IC&S that no random or regular audits of ADAMA, ACC PROMIS or ACID/ALEIN use or access are conducted by the ICT section. Reactive audits are done to investigate suspected breaches.

2.99 From September 2008, in response to the identification of some documents with incorrect access controls, the Planning and Governance Section conducted both regular and random access control audits on ADAMA in relation to high risk or sensitive information or individuals, as well as specific audits on request.

The Random Audit Program

2.100 The ACC has a Random Audit Program whereby Senior Executive Service (SES) officers conduct a program of random audits of their own or other ACC state offices. General Managers inspect investigators' Official ACC Diaries and Notebooks and check that they have been reviewed and signed off by team leaders or managers. The *Management and Supervision of Seconded Police Investigators and ACC Contract Investigators Policy* sets a standard of regular and at least monthly review of Official ACC Diaries and Official ACC Notebooks. The SES officers also check vehicle logbooks and do interviews called *Organisational Health Checks*. These health checks are interviews with staff to seek feedback on a range of

organisational issues and the ACC Values. They are forwarded to the Manager Compliance for collation and are reported to the ACC Audit Committee.

2.101 At interview, an ACC senior investigator advised us that he regularly audited Official Diaries and that his own diary was signed off each month by his supervisor. We sought to interview another investigator who was asked to furnish their Official Diary and Official Notebook for our inspection, however that investigator declined to be interviewed. This is discussed further in the section on seconded police officers.

2.102 Our investigation found that the most recent Random Audit Reports covered the periods September–October and November–December 2008. The reports indicated that 24 diaries were checked; two of these diaries were not up-to-date and five did not meet standards for correct checking or oversight by area supervisors. In December 2008, two diaries had not been inspected in the preceding six to eight months. Follow up action was documented. We discussed the Random Auditing Program with the Manager Compliance, the General Manager People, Standards and Security and the Chief Auditor.

2.103 In response to enquiries raised by our investigation, our review team was provided with an analysis, produced in July 2009, of the number of random audits conducted between September 2005 and May 2009. December 2007 to December 2008 was the most prolific period for the completion of random audits. A small subset of SES officers produced the majority of the completed audits.

2.104 We then examined ACC internal communications for September 2008, December 2008 and June 2009, reminding senior staff of the importance of completing the audits. We were not provided with Random Audit reports for the first half of 2009.

2.105 In our view, the Random Audit Program offers an effective communication channel between staff and senior management and the opportunity for an important integrity check of an investigator's information collection via Official ACC Diaries. The audit program is restricted, however, by competing management responsibilities of SES officers, and reporting has been delayed by the compliance area which had also been engaged in the investigation of recent breaches and had significant policy and program redesign tasks.

Recommendation 5

The value of the Random Audit Program should be confirmed by the Executive and the program should be renewed with regular audits and current reports. It may be appropriate to consider devolving audit collection to another level of management and reviewing the collation and reporting task.

Operational audits and corruption resistance reviews

2.106 ACC Professional Standards and Compliance developed and, in 2007, rolled out a new program of Operational Audits and Corruption Resistance Reviews. Professional Standards and Compliance has conducted 20 Operational Audits and 17 Corruption Resistance Reviews since February 2009.

2.107 Operational Audits examine a staff member's understanding of, and compliance with, procedures and policies in areas such as exhibits handling and covert source management. Corruption Resistance Reviews are based on the New South Wales Independent Commission Against Corruption model. They comprise

guided interviews with a staff member to examine and reinforce knowledge of, and compliance with, the rules and guidelines for secondary employment, conflict of interest, and gifts, benefits or bribes.

2.108 In our view, these audits and reviews are important and demonstrate to staff the agency's commitment to maintaining an integrity culture.

The Information Technology Security Adviser role

2.109 The April 2009 Deloitte report on the review of ACID/ALEIN observed that the IT Security Adviser (ITSA) role in the ACC was much smaller than the *Australian Government Information & Communications Technology Security Manual* prescribed. At interview we were advised that the ACC has begun to redevelop the ITSA role. This position will be upgraded from a half-time to a full-time position and will report directly to the CIO.

2.110 We were advised that the previous ITSA, previous Acting CIO and previous CIO had not communicated well. As a consequence the then ITSA was not included in the oversight of, or given access to, the IT audit logs.

2.111 We interviewed the current ITSA, who impressed us as a committed and engaged IT professional. The ITSA valued the recent change to line reporting to the CIO.

2.112 Access and management of database audits is an important aspect of the ITSA's role. During this investigation it became apparent that with the exception of the ADAMA random audits by Planning and Governance from September 2008, no random audits of any of the ACC's databases were conducted, although users apparently believed that they were conducted. The ITSA had conducted access audits in response to recent information disclosures.

2.113 The ITSA advised our investigation that a broad-based program of random audits of staff database access would not be the most productive use of resources. His view was that random IT access audits would be time consuming, and the ITSA would be hindered by needing to know what it was appropriate for each randomly-audited staff member to access.

2.114 We put specific queries related to possible audit functions to the ITSA. In response to our queries we were advised that:

- random audit of System Administrators access logs (i.e. ADAMA, ACID) is important, and was currently not done
- there was no current audit function to record a user's database search items to enable an audit of any user's browsing
- random audits of access logs for specific database entities was important and was not routinely done; this facility could be used to check on a user's access to, for example, database lists of members of organised crime groups
- ADAMA did not currently enable a retrospective document print audit; this facility could be implemented and should not be expensive
- staff are advised that USB drives are not able to be connected to ACC personal computers (PCs) and that they cannot be used to make a copy; however, USB devices can be connected to some ACC PCs and could copy material and USB drive access control was weak. This could be improved to allow ACC-certified USB drive use and access control

- all audit logs could be removed to a central database and format. This would improve audit-log security and would provide greater access control to these logs. This is an important issue as tamper-resistant or immutable audit logs are an important tool when attempting to verify unauthorised access
- ADAMA Incident Reporting pathways were undeveloped; it would be useful if the ITSA role was developed as a joint ITSA and ICT Security Professional role (with a hands-on administrator role).

2.115 Separately, we were advised that TRIM/ADAMA administrators previously performed regular search audit logs of their administrator activity (Active Audit Events) and saved the logs for later integrity checking, but that this practice had ceased.

2.116 The Ombudsman notes the risk that the ITSA's attention may be diverted to other ICT administrator tasks, given that the number of ACC ICT staff has been reduced, and that the ITSA has a current additional role as the ACC Citrix Administrator.

2.117 We understand that the ACC is considering a method, or staff position, to improve the coordination of ICT security between the CIO, the ITSA, the ACID Business Manager, the Manager Standards and Security and, at times, the Manager Professional Standards. The Ombudsman notes the importance of developing an effective formal communication and coordination strategy or structure for this professional group. During interviews we noted that the ITSA, CIO and ACID Business Manager appeared to hold common views and shared an understanding of the needed system improvements.

Recommendation 6

The ACC Executive should consider improving the ACC's ICT audit and incident reporting systems, as discussed in this report.

Building an ethical culture

Induction program

2.118 The ACC has invested in improving its induction program and management training. The Learning and Development section has created an online induction guide with an online staff sign-off, so that the agency can ensure, and record, that all new staff receive a timely and consistent induction.

2.119 Under the induction program all staff receive a security briefing—state staff from their local office manager and Canberra staff from the Manager Standards and Security. We examined the ACC Induction Security Briefing dated December 2008. This provides a good introduction to security practices and, in particular, physical and document security and document security classification and handling. The briefing mentions the need-to-know principle.

2.120 In our view, the ACC Induction Security Briefing could be further enhanced by:

- explaining the s 51 secrecy provision
- describing the need-to-share and need-to-know continuum, and expounding the ACC's policy position on this

- explaining access-control measures for database documents
- explaining the role of the IT Security Adviser
- describing and defining information misuse and information access breaches, and the sanctions
- providing a more defined incident reporting process for suspected ICT and information security breaches.

2.121 An enhanced Induction Security Briefing may require more time than the current one-hour program. The Learning and Development section advised that a video conference briefing by the Manager Standards and Security was mooted and this could provide greater consistency and information currency in this critical area.

Professional standards and compliance

2.122 The ACC is promoting adherence to the APS Values and Code of Conduct via the new *Professional Standards and Integrity Management Plan 2008–2009*, and the revised *Fraud Control Plan 2009–2011*.

2.123 The Professional Standards and Compliance area comprises the Professional Standards and Compliance Managers. Both are key integrity culture positions for the organisation and report to the Manager People, Standards and Security. These managers have designed and delivered ethics training for all staff. They also developed the *Draft Workplace Behaviour Policy* covering underperformance, workplace conflict and promoting the active resolution of issues by line managers.

2.124 The current complaints policy states that ACC staff should report any allegations of improper or illegal conduct. The new draft policy provides that staff have an obligation to report misconduct. Staff may report misconduct to their supervisor, any manager or the Manager Compliance and Manager Professional Standards.

2.125 This policy is supported by a *Draft Workplace Behaviour Policy and SOP* which reinforces the Code of Conduct and ACC Values, including—'to handle, store, share and disseminate information appropriately'.

2.126 The Manager Compliance manages the investigation of Code of Conduct breaches and draws assistance from the Manager Professional Standards as required. The Manager Professional Standards has a police and police integrity background and has been with the ACC for 14 months. This background is relevant given the presence of secondees from police services and of ACC covert investigation officers, and the importance of influencing the behaviour of those officers. The CEO, the Executive Director Organisational Services, the General Manager People, Standards and Security, the Manager Professional Standards and, at times, the Manager Compliance hold weekly meetings to manage integrity issues.

2.127 The Draft Workplace Behaviour Policy is linked to the ethics training program. In 2008, Professional Standards rolled out a new program of ethics training and since late 2008 has delivered 16 ethics training courses for ACC staff in five states. These courses develop awareness of ethical issues, information security and corruption prevention, the ACC Values, the Code of Conduct, and the reporting and disciplinary processes for breaches. A senior operational manager advised that the Professional Standards ethics awareness training did influence the seconded investigators and that induction had significantly improved.

2.128 The education programs of the Learning and Development Section and those conducted by Professional Standards and Compliance appear to effectively complement the ACC's integrity culture building program.

The ACC staff culture

2.129 Throughout the interviews which we conducted for this investigation, we were assisted by ACC staff who appeared to be committed to their roles, to be diligent, and who were frank and reflective in reporting on the ACC's situation. Staff were focused on developing intelligence on, or investigating, serious and organised crime.

2.130 At interview, some staff expressed disappointment and felt 'betrayed' by recent information leaks—morale was affected. We were told by staff that, in their view since the investigation into the leak of ADAMA 08/4610, any breaches of procedures by lower-level staff were treated more seriously than the treatment of the SES officer in that case. Staff reported that they lacked information about what action had been taken but said that the SES officer had not been sanctioned to the same degree as they would be in similar circumstances. The Manager Professional Standards advised that similar views were raised by staff attending the ethics training sessions.

2.131 This presents an important aspect of the effective investigation and sanction of breaches and raises an issue for ACC senior management. Should that impression remain, it could work against efforts to enhance the ACC's integrity culture. There is a risk that staff sympathy may lie with future lower-level staff who breach information access rules and therefore disclosure or reporting may be reduced.

2.132 Clearly, there are privacy issues in relation to disseminating information about sanctions of the ACC which can be amplified in a smaller organisation. In our view, there needs to be sufficient confidentiality to enable appropriate, lawful and fair investigation. Then, having determined a breach and imposed a sanction, there needs to be a mechanism for reasonable, adequate disclosure to demonstrate that breaches of rules are followed and sanctioned in a fair manner. Such a process builds compliance.

2.133 The ACC is not bound by the *Privacy Act 1988* (Privacy Act) due to the operation of s 7 of that Act. However, the ACC has a policy of abiding by the Privacy Act as far as possible.

2.134 The Public Service Commissioner has produced a circular that provides guidance on disclosure of personal information regarding misconduct where 'it is necessary, appropriate and reasonable to do so'.[5] The principles outlined relate to balancing issues such as: the nature and seriousness of the misconduct, the aim of the disclosure, the prevalence of the type of misconduct and the need to highlight particular cases for education deterrence or prevention, and the employee's right to privacy. The circular notes that it may be appropriate for senior management to advise all staff, in a general way, about recent finalised cases of breaches of the Code of Conduct and the sanctions applied.

2.135 The Ombudsman recommends that unauthorised information access be considered a serious breach of the ACC policy which should be sanctioned as such. The Ombudsman recommends that the ACC should ensure that staff members are

---

[5] Circular No. 2008/3: *Providing information on Code of Conduct investigation outcomes to complainants*, Australian Public Service Commission.

aware of information access rules and their responsibilities. Policies advising staff could also warn that information about breaches of the Code, and the sanctions applied, will be provided to all staff in a general form as an aspect of maintaining a culture of integrity.

Management of seconded police officers

2.136 The ACC Act provides for the secondment of officers from the AFP and state police forces. They are often employed as ACC investigators and may be involved in complex investigations that involve significant risks to them and to the organisation.

2.137 The ACC has developed a process whereby it obtains an assurance from the senior police officer of the relevant external law enforcement agency that the proposed seconded officer is not under suspicion of integrity breaches, and from the relevant integrity oversight body that the officer is not a person of concern.

2.138 The ACC's culture and integrity building program has centred on promoting the APS Code of Conduct. Newer policies state that all policies and the Code of Conduct apply to all ACC staff employees. Seconded police officers become members of the staff of the ACC, but they are not APS staff and are not able to be sanctioned under the Public Service Act for breaches of the Code of Conduct.

2.139 The *Draft Complaints Management Framework Policy and SOP: Management of Complaints and Misconduct* at point 5.1 acknowledges this. This policy resolves the issue by enabling the Manager Compliance to conduct preliminary enquiries and then refer the matter to the CEO, and the Executive Director Organisational Services, to consider whether the home agency or the ACC will investigate the matter. Ultimately, the recourse is to send the seconded police officer back to their home agency with advice to the head of that agency of any alleged misconduct.

2.140 The ACC has developed processes to expedite notification, by the ACC CEO, of police officers suspected of corruption to their respective police commissioners, integrity commissions and the Australian Commission for Law Enforcement Integrity (ACLEI).

Refusal to be interviewed

2.141 In the course of this investigation we sought to interview ACC staff and seconded officers at an ACC state office. Given the time frame of the investigation we provided three to four business days' notice of our intention to interview staff. One ACC seconded police officer first sought advice from their police association and then declined to be interviewed. We contacted their superiors and contacted the investigator by email.

2.142 We surmised that the seconded staff member may not have been given an adequate explanation of our investigation and our purpose. Therefore, we provided the seconded officer with a written, clear explanation of the investigation and the protection afforded to them by the *Ombudsman Act 1976*. We advised them that it was not a complaint about themselves, that their CEO had requested the investigation, and they had been selected by their management to assist our investigation and that we wished to interview them.

2.143 The seconded officer stated they had sought legal advice and declined to be interviewed unless they were directed to do so by their management. If so directed, they advised they would again seek their police association's advice.

2.144 This response contrasted with the cooperation and the frank and thoughtful responses provided by other interviewed ACC staff. It also serves to highlight the risk that seconded officers, while being members of staff of the ACC, may not see themselves as ACC staff and behave accordingly.

Management of higher-risk employees

2.145 Disgruntled employees are recognised in the ICT literature as a foreseeable and serious potential risk to an organisation's information integrity. The ACC has developed a draft Workplace Behaviour Policy that emphasises the ACC Values and expected behaviours to reinforce integrity and accountability, and has introduced a drug-screening program.

2.146 The General Manager, People, Standards and Security, and the Manager Compliance advised that, when considering a member of staff under suspicion or investigation for a suspected information breach, the decision about when to restrict access to information holdings is made in each case after consideration of the circumstances. To restrict access at an early stage may serve to inform a person that they are the subject of an investigation, either internally or by ACLEI, and prejudice that investigation. This had to be balanced against the risk afforded by their level of access to information holdings.

2.147 The *Draft Management of Complaints and Misconduct Policy* supports this management and provides, at point 8.4, for temporary reassignment or suspension of duties at any time while determining if a breach of the Code of Conduct has occurred.

2.148 The managers provided two recent examples where the ACC restricted access to information for people who were under investigation for suspected breaches of professional standards. In one case the staff member was moved to a low risk project (however they retained general ADAMA access). In another, when the staff member was given advice of the decision to terminate, they were also stood down from duty pending termination or appeal.

2.149 There may be situations in which an employee is known to be disgruntled but is not under suspicion or investigation for a Code of Conduct breach. These employees may present an integrity risk but the ACC does not seem to have a policy to monitor their behaviour. We draw this matter to the attention of the ACC for further consideration.

ANNEX 1—INTERVIEWS CONDUCTED

External

- Robinson Review, Mr Martin Brady AO
- Office of the Inspector-General of Intelligence and Security, Ms Rachael Spalding.

ACC Canberra office interviews and telephone/teleconference

- Executive Director, Organisational Services
- Executive Director, Programs
- Acting Chief Information Officer
- Manager People Capability, Learning and Development
- Manager Professional Standards
- Manager Standards and Security
- Manager Intelligence Capability and Support Services [and de facto Manager ACID/ALEIN]
- Information Communication Technology Security Adviser
- General Manager, High Risk Crime Groups
- Principal Specialist, Strategic Intelligence Team
- Deloitte Touche Tohmatsu, Mr Craig O'Hagan and Mr Shawn Willis (at initial interview)
- Systems Training Specialist
- Risk Adviser
- Manager Business Management and Reporting
- Manager, Financial Intelligence Assessment Team
- Manager Compliance (Professional Standards)
- General Manager, People, Standards and Security
- Manager, Board Secretariat
- Senior Auditor
- TRIM/ADAMA Administrator.

ACC Sydney office interviews

- Team Leader, Intelligence Capabilities & Strategies
- Intelligence Analyst
- Head of Determination/Operations Manager
- Senior Collections Analyst
- Investigator and former Assistant Head of Determination.

ACRONYMS AND ABBREVIATIONS

ACC	Australian Crime Commission
ACC Act	*Australian Crime Commission Act 2002*
ACC PROMIS	ACC case management database
ACID	Australian Criminal Intelligence Database
ADAMA	ACC main document database; TRIM based
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
ALEIN	Australian Law Enforcement Intelligence Net (network that connects LEA users to ACID)
APM	Australian Police Medal
APS	Australian Public Service
CIO	Chief Information Officer (ICT)
CNZM	Companion of the New Zealand Order of Merit
Code of Conduct	APS Code of Conduct
Deloitte	Deloitte, Touche, Tohmatsu—consultants
FIAT	Financial Intelligence Assessment Team
FOI	*Freedom of Information Act 1982*
HoD	Head of Determination
ICT	Information communication technology
ITSA	Information Technology Security Adviser
KPMG	KPMG consultants
LEA	Law enforcement agency
MOU	Memorandum of Understanding
NCIPs	National Criminal Intelligence Priorities (ACC)
SES	Senior Executive Service (APS senior officer)
SFCIN	Suspected Financial Crimes Intelligence Network
SOP	Standard operating procedure