Inquiry by the Parliamentary Joint Committee of Public Accounts and Audit

Management and Integrity of Electronic Information in the Commonwealth

Submission by the Australian Crime Commission January 2003

Table of Contents

Glossary

ATO	Australian Taxation Office
ABCI	Australian Bureau of Criminal Intelligence
ACC	Australian Crime Commission
AFP	Australian Federal Police
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
CLEB	Commonwealth Law Enforcement Board
COE	Council of Europe
Customs	Australian Customs Service
Cyber-forensics	Application of computer and digital technological systems investigation and analysis for determining potential evidence
DSD	Defence Signals Directorate
Email	Electronic mail
HOCOLEA	Heads of Commonwealth Operational Law Enforcement Agencies.
Internet	The vast collection of inter-connected networks that all use the TCP/IP protocols
Intranet	A private network inside a company or organisation, similar in principle to the Internet
IT	Information Technology
LAN	Local Area Network
LEA	Law Enforcement Agencies
MOU	Memorandum of Understanding
NCA	National Crime Authority
OECD	Organisation of Economic Co-operation and Development
PSM	Commonwealth Protective Security Manual 2000
SGE	Secure Gateway Environment – a DSD certified secure extranet gateway provided by 90East

1 Introduction

With the commencement of the Australian Crime Commission (ACC) on 1 January 2003, the functions of the former National Crime Authority[1], Australian Bureau of Criminal Intelligence[2] and Office of Strategic Crime Assessments[3] were brought together in a national level agency tasked with the provision of a criminal intelligence service to the Australian community and law enforcement. The specific functions of the ACC include to-

- provide advice to the ACC Board on setting national criminal intelligence priorities;
- collect, correlate, analyse and disseminate criminal information and intelligence (including maintenance of a national database of that intelligence);
- undertake authorised intelligence operations (including use of ACC special powers where approved);
- undertake authorised investigations of federally relevant criminal activity (including use of ACC special powers where approved); and
- provide strategic criminal intelligence assessments to the ACC Board.[4]

It is worth noting that the provisions of the ACC legislation relating to secrecy, FOI and protection from disclosure will apply also to the information and intelligence inherited from the ABCI and OSCA functions, as well as the ongoing collection of material under those functions.

As with much of the information and intelligence contributed to NCA national task forces in the past, much of the criminal information (placed on the ABCI ACID database) and intelligence (published to agency staff with access via the ABCI's ALEIN network desks) provided to the ABCI has been contributed by State and Territory Police Services, and was provided explicitly or implicitly for specified purposes, and subject to restrictions on disclosure beyond partner law enforcement agencies.

In the case of the national task forces coordinated by the NCA, a large amount of information and intelligence has been provided by participating task force agencies for the purposes articulated in the national management plans (classified) for those task forces and as the task forces were formed under the NCA Act, with task force members being "members of staff of the NCA, information flows were facilitated across task force members but were largely restricted from further dissemination.

1 An agency formed under the *National Crime Authority Act 1984 (Cwlth)* and with underpinning legislation from all States and Territories. It had statutory functions, and to protect its information security and the reputation of persons under investigation, the NCA Act contained secrecy provisions covering all "members of staff" (included seconded police and members of NCA task forces), the ability to protect its information and intelligence from disclosure, limitations to FOI provisions and exemption from the operation of the Privacy Act (Cwlth)

2 one of the common police services answerable to a Board of Control comprising Police Commissioners

3 an element of the Attorney-general's Department preparing national level over-the-horizon strategic law enforcement intelligence

4 Section 7A, *ACC Act 2002*.

The Australian Crime Commission (ACC), like other Government agencies, will collect, process, store and disseminate a range of electronic information both internally and to its clients. This information can be in written, audio and visual form. Since the establishment of the forerunner to the ACC, the National Crime Authority (NCA) in 1984, new technologies have changed the way information is collected and used by both law enforcement agencies (LEA) and criminal enterprises. While it is recognised that these technologies have enormous benefits, they introduce a risk to the care and custody of that information.

The ACC also operates an Internet site, for the purpose of publishing information about the agency, such as annual reports and media releases. In terms of the Commonwealth Government's Investing for Growth policy, this site is a Stage 1 Site. That is, it is a static site which does not allow interaction with the agency's databases or the exchange of sensitive information. Given the nature of the ACC's operations, it is not anticipated that the Internet site will evolve to a non-static site.

The Internet is utilised by ACC staff for research and the collection of open source information. This is through a series of DSD certified firewalls known as the Secure Gateway Environment (SGE) operated by 90East. [5]

ACC staff use email for the exchange of information between elements of the ACC, other Government agencies and Commercial organisations both National and International.

The ACC has an internal capacity to identify and utilise new technologies and information processing capabilities that will assist investigations into complex national organised crime. In relation to this, the ACC is developing newer electronic information processing platforms continually (e.g. the ALERT program … forensic techniques)

The ACC, like other Commonwealth agencies and State and Territory Law enforcement agencies is subject to an extensive range of legislation to protect the privacy, confidentiality and integrity of information entrusted to it. Although exempted from application of the *Privacy Act 1988* (Cth), the ACC seeks to ensure that the spirit of the legislation is met and that the collection, use, storage and dissemination of information is subject to appropriate controls and safeguards. The ACC also collects, uses, stores and disseminates information in line with the Commonwealth Protective Security Manual 2000 (PSM) to protect the integrity of its electronic data.

As with its forerunner agencies, the ACC will continue to maintain and develop a secure database, intelligence publication desks, and other systems in support of law enforcement agencies, subject to the secrecy and dissemination regime in the ACC legislation.

[5] 90East is a registered company who operate a certified gateway by DSD

2 Terms of Reference: Confidentiality of Information

The privacy, confidentiality and integrity of the Commonwealth's electronic data.

As indicated above, the ACC manages a range of information for a number of reasons, including the investigation of complex national organised crime, the administration of the agency and security considerations. Information collected across the functions of the ACC is to assist in describing the threat from serious and organised crime, and developing opportunities to respond to that threat, which frequently extends across, indeed exploits, domestic and international jurisdictional boundaries. As such the information will not be restricted in either its collection or use, to Commonwealth purposes.

The reasons for collecting information in future will mostly relate to national intelligence priorities settled by the ACC Board, but will also extend to support of individual partner agency policing activities (including provision of primary information and intelligence databases for agencies), and the identification of emerging threats. This scope will extend beyond merely Commonwealth interests, encompassing information in relation to offences against State/Territory legislation, or links to overseas partner agency activities.

The information dealt with by the ACC may relate to suspected criminal activity by Australian citizens, law enforcement investigative methodologies, or the personnel details of investigators. It is therefore crucial that this information is managed with appropriate confidentiality and integrity. This information may be classified in accordance with the PSM.

The ACC is required, pursuant to the PSM, to obtain and hold information which facilitates the security clearance of all staff. Such security clearances ensure that only those staff deemed suitable have access to sensitive information. The PSM additionally requires the ACC to ensure the physical protection of its sites and staff, hence this information may also be classified.

Within the IT applications environment, processes are in place to periodically examine the integrity of classified data under ACC control (verification of links, associated data and quality control)

Privacy, integrity and confidentiality of Commonwealth Electronic Information cannot be guaranteed outside the boundaries of the Commonwealth due to jurisdictional differences in legislation, policy, terminology and standards, eg different data schemes and classifications.

There are boundary issues as to what is Commonwealth Information, eg a joint task force operation may see operational data stored on other jurisdictions' systems depending on individual task force arrangements.

The integrity and quality of data transmitted from the source is often assumed but not validated, eg from telecommunications carriers.

The volume of data being managed continues to grow, quality can be variable and challenges exist to manage, filter and analyse data.

3 Terms of Reference: Electronic Transmission

The management and security of electronic information transmitted by Commonwealth agencies.

For the purposes of this submission, 'electronic transmission' describes the electronic transfer of information within and between law enforcement agencies rather than in person or through paper documents. Transmission can be via networks, email, radio, floppy disks etc.

The Board of the ACC[6] and the Chief Executive Officer of the ACC[7] are empowered to disseminate to Australian and international law enforcement agencies, or to any other agency or government body, strategic criminal intelligence assessments.

Where information is transferred electronically to other Commonwealth agencies, those agencies have the appropriate management and security practices in place, as required by the PSM.

Where the ACC disseminates classified information to non-Commonwealth agencies (as with the NCA and ABCI previously), settled arrangements (relating to the task force frameworks) or other agreements will specify the technical security and administrative arrangements relating to transfer of information not the subject of formal disseminations of information under the ACC Act. Special arrangements will continue to be made in relation to particular classes of restricted access information such as electronic surveillance product, ATO and AUSTRAC information. Whilst State and Territory agencies are not subject to the PSM, they and their nominated staff with access are bound by the general conditions of access to the ACC information, and any additional special conditions placed on particular information disseminations. This information may be used for a multitude of functions including:

- Intelligence analysis
- Investigation and prosecution of crimes
- Administration of the organisation
- Security management

The ACC currently operates within a secure national network that links all its offices and is encrypted according to Defence Signals Directorate (DSD) requirements. Additionally, the ACC national network is part of a Federal Government electronic environment that operates secure encrypted links between a number of other Commonwealth agencies. An extension of the

[6] Section 7C(g) of the *ACC Act 2002*.
[7] Section 59(7) – (11) of the *ACC Act 2002*

ACC network provides links to State and Territory jurisdictions where the secure links are under Commonwealth management. The encrypted national network ensures that information exchange between the ACC and key partner agencies, such as the Australian Federal Police, occurs in a protected environment, safe from the risk of unauthorised access. This exchange of information may be via various applications or by email.

The ACC security and information management policies and practices are undergoing review as the ACC commences operation, to ensure that those policies encompass the requirements of the PSM and of the new ACC.

As with the former ABCI, the security of data transmitted electronically to the ACC from other agencies will continue to be in accordance with settled security and administrative protocols which are in the process of integration across the ACC is assumed to be in place, i.e. before it enters our secure network.

4 Terms of Reference: Storage and Network Architectures

The management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks.

The ACC stores and processes information on a number of IT systems in geographically distributed environments. The major systems are centrally controlled and managed, however individual work areas may hold information locally.

These IT systems have been developed to meet the operational and administrative needs of the ACC. Management of the information held on these systems is primarily controlled by the functional areas while the systems themselves are predominately managed by the IT Branch. Two of the primary operational/intelligence systems are managed outside of, but in consultation with IT Branch:

- NCA PROMIS case management system (administered for the NCA by the AFP but separate to AFP PROMS)
- ACC TI RADARS system is administered by TI Section

Security oversight is maintained by several areas including IT Branch and the Security Group.

There is a need to accommodate common data repositories, standards etc to eliminate duplication or inaccuracy.

5 Terms of Reference: Legislative and guidance frameworks

The adequacy of the current legislative and guidance framework.

There is a range of Commonwealth legislative and guidance documents prescribing the ACC's requirements for the management and security of information. The Commonwealth legislative framework the ACC operates within includes but is not limited to:

- ACC Establishment Act 2002 (Cwlth)
- ACC Act 2002 (Cwlth)
- ACC State/Territory Provisions legislation (yet to be passed)
- Telecommunications Act 1997
- Telecommunications Interception ACT 1979
- Crimes Act 1914
- Cybercrime Act 2001
- FOI Act 1982
- Archives Act 1983
- Privacy Act 1988
- State and Territory legislation regarding the collection and management of information using warrants (eg listening devices, surveillance devices, controlled operations)

The primary Commonwealth guidance documents utilised by the ACC are:

- PSM 2000
- DSD ACSI 33 and 37
- ACC Policy and Procedures Manual (classified)

The ACC came into operation on 1 January 2003. As part of the transition, process, internal policies and procedures manuals will undergo review and redevelopment to ensure suitability and relevance.

Additionally there is a range of various State legislative and guidance documents prescribing the ACC's requirements for the management and security of information entrusted to it. Some of these guidance documents for the classification and handling/release of State based information have different requirements in particular where the naming standards are identical to the Commonwealth e.g. CONFIDENTIAL and SECRET. Also State and Territory legislation.

6 National Co-operation - Mutual Recognition of Classification Standards

The current patchwork of Commonwealth, State and Territory information management practices creates investigative difficulties when information needs to be obtained/disseminated in a number of jurisdictions in the course of the one or more operations. For example a multi jurisdiction Task Force may require that ACC information be shared to facilitate the efficient and successful investigation of criminal activities. Elements of this information by default will be classified under the PSM standards for information management. This is a particular problem for the ACC investigations that have a national and international focus. In the past, national task force members have been subject to the secrecy and other provisions of the NCA Act applying to "members of staff".[8] This will continue under the ACC legislation, although the scope and purpose of task forces established by the Board may be different to the previous NCA task forces.

A distinction should be drawn between the facilitated disclosure of information under task force arrangements to task force members for the purpose of a task force investigation or intelligence activity on the one hand, and formal dissemination to another agency for a specific purpose or general use on the other. The later will continue to require formal dissemination under Section 59(7) to (11) of the ACC Act by an ACC officer delegated by the ACC CEO for that purpose.

The ACC considers that there is a need for a co-operative information management scheme that would allow for the electronic exchange of information in a timely manner. This scheme would need to ensure that minimum standards are set and maintained similar to those the ACC is required to comply with.

This co-operative arrangement may be most appropriately dealt with by way of legislation rather than by administrative arrangement. While the ACC preference is for national standards, it would be an advantage if individual States and Territories implemented a scheme of mutual recognition based on the PSM. The scheme could involve reporting compliance to the relevant Attorney-General or an-Australian National Audit Office type authority.

As stated earlier, the ACC currently operates within a secure national network that links all offices and is encrypted to DSD requirements. Additionally, the ACC is part of a Federal Government environment that has secure encrypted links to a number of other Commonwealth agencies. An extension of this ACC network provides links to State and Territory jurisdictions where the secure links are under Commonwealth management.

[8] See definition of "member of staff" in Section 4 of both the NCA Act 1984 and ACC Act 2002

7 International Co-operation

The need for international co-operation in the form of mutual assistance has never been greater. Many ACC investigations have an international aspect, which may involve the ACC seeking the co-operation of overseas law enforcement agencies, through AFP Liaison Officers or formally gathering evidence pursuant to the *Mutual Assistance in Criminal Matters Act 1987.*

The importance of international co-operation is emphasised by the development of the Council of Europe (COE) Draft Convention on Cyber-crime. The COE is a 41-nation organisation concerned with combating money laundering. Due to the importance of the issue, non-member States, such as Canada, Japan, South Africa and the United States actively participate in negotiations. The aim of the convention is 'to harmonize national legislation in this field, facilitate investigations and allow efficient levels of co-operation between authorities of different States'. The Draft Convention addresses this in respect of matters such as offences against computer data and systems, copyright offences, search and seizure of computer data, interception and mutual assistance.

As many computer crimes have an international dimension, national measures need to be supplemented by international co-operation. The exchange of information including classified information therefore needs to be under an information management and security umbrella for the mutual protection of all agencies' information.

Australia is committed to the principles of the Draft Convention. In May 1999, the Law Ministers of all Commonwealth countries mandated the Commonwealth Secretariat to convene an expert group to draft a model law for use by Commonwealth countries with reference to the Draft Convention. The ACC understands that this work is ongoing.

Related work is also being undertaken by other international bodies, including:

- United Nations (eg. Workshop on Crimes related to the Computer Network).
- Organisation for Economic Cooperation and Development (OECD).
- Interpol (eg. International Conference on Computer Evidence).

The ACC submits that there is a growing need for the development of mutually recognised standards for the electronic protection of LEA information.

Current impediments to effective international law enforcement co-operation will be exacerbated by the challenges posed by speed, nature and extent of new technologies. The ACC acknowledges that steps are being taken to address this, such as the Draft Convention of the COE. Harmonisation of

laws regarding gathering evidence in computer crimes that cross international borders, mutual assistance and extradition are important. This is a long-term process requiring sustained prioritisation and support.

With the growing focus on counter terrorism, this need for cooperation, exchange of information in a timely manner and the mutual protection of that information can only grow in importance.

Management of information:

It would be useful to map out the dissemination and secrecy provisions across law enforcement agencies and particular types of restricted information in each jurisdiction

It should be noted that depending on the source of information, law enforcement agencies are required to comply with legislative requirements pertaining to the collection, storage, use, dissemination and destruction of particular types of information. Some of this information may have a number of sources some of which are so restricted and some not.

The ACC will continue to place appropriate restrictions on specific disseminations of information.

8 Conclusion

Development and enhancement of settled national information exchange standards, protection, and systems remains an essential capability underpinning the role of the ACC as it was for its predecessor agencies.

The Commonwealth as well as LEAs must have a comprehensive and secure electronic information management system to enable agencies like the ACC to keep pace with new and emerging technological developments and consequent changes in investigative and criminal methods. Given the Globalisation and Transnational nature of organised criminal enterprises, there is a need for a national and international set of information management and security standards for the protection of this information; to enable the agency to work with partner agencies to a common set of standards and facilitate the exchange of electronic information in a secure and timely manner.