Australian Federal Police
To fight crime together and win
ABN: 17 864 931 143

18 December 2002

The Secretary
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Secretary

INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

In response to your correspondence of 28 October 2002 to Commissioner Michael Keelty, the following information is provided.

The Australian Federal Police has developed and implemented policies, standards and procedures to ensure the efficient management and the integrity of the electronic information in its care. A general principle is that the protection of the AFP's official information, its assets and personnel is the concern and duty of every member and staff member of the AFP, regardless of their rank and status. This is an overarching principle which guides the AFP's ongoing activities in the areas listed below:

- Compliance with Commonwealth privacy policies and copyright guidelines.
- IT and communications security to protect electronic information and IT systems from intrusion, corruption and loss
- Security Vetting of Personnel
- Physical Security and Risk Management
- IT Threat and Risk Assessment and Business Continuity planning
- Internet and Intranet publishing
- Electronic and paper based records management
- E-business and communication with Government Agencies, private organisations and the public.
- Compliance with Government polices and standards relating to the above issues.

To ensure the physical security of data systems and other assets the AFP, under its National Policy on Security and Information:

- maintains and monitors implementation of the AFP Security Plan;
- maintains and monitors implementation of the AFP Risk Management Plan;
- conducts proactive, periodic security threat and risk reviews supported by appropriate remedial action;
- adheres to an internal audit program that identifies risks associated with physical security, administrative procedures, personnel and operations, and monitors remedial action;
- maintains and monitors implementation of the AFP Fraud Control and Anti-Corruption Plan;

- audits AFP IT networks, and monitors the use and integrity of IT systems;
- complies with relevant provisions of the Commonwealth Protective Security Manual;
- ensures that all personnel undergo security clearance before they are exposed to classified or sensitive material;
- investigates all suspected breaches of security;
- instils an awareness of security through education and training;
- maintains a viable, reliable and technologically proficient AFP network;
- applies the provisions of the Privacy Act 1988 and Government policy relating to the protection of privacy; and
- releases information in accordance with the Freedom of Information Act 1988.

In 2001 AFP Internal Audit, in consultation with AFP Information Technology, sponsored a thorough risk assessment of the AFP's in-house IT Security situation, which addressed the main issues raised in:

- the Commonwealth Protective Security Manual (2000),
- Australian Communications – Electronic Security Instructions (ASCI 33), and
- AS/NZS ISO/IEC 17799:2001 Information Technology – Code of practice for information security management (which superseded AS/ANZ 4444).

The results of the risk assessment were reported in February 2002 and identified a number of actions that needed to be taken. While many of the higher residual risks were already recognised by the AFP, their treatment represents a significant undertaking for the AFP. The AFP's Audit Committee, known as the Security and Audit Team, is monitoring progress against these recommendations.

The following policies, standards and procedures have been developed and implemented to support the above activities:

Australian Federal Police Protective Security Manual (AFPPSM)

The AFPPSM details the policy, standards, responsibilities and security organisation to be adopted for the application of protective security measures within the Australian Federal Police. The six volumes of the manual form the basis upon which Team Leaders/Managers at all levels develop security plans to implement and maintain an acceptable standard of security for the protection of official information, assets and personnel under their control. The policy and standards of this manual apply to all employees of the Australian Federal Police.

It includes an introduction to overall AFP security policy, organisation and administration, as well as policy, standards and procedures for the

- protection of official information,

- security vetting and related personnel security requirements,

- planning, acquisition, installation, commissioning and operation of information and communication systems,

- physical security measures and administrative controls for the protection of AFP premises, installations, facilities and assets, and

- reporting and investigation of breaches of security and security related incidents and the conduct of security surveys, inspections and checks

Information Technology Security Policy Statement

The aim of this policy statement is to set out the policy and principles for the establishment of information technology security strategies to achieve the appropriate levels of protection, availability, reliability and integrity for AFP IT systems and data. It covers security responsibilities, legislation, regulations and policy, education and training, information security, electronic mail, AFP Intraweb, Internet, software, hardware, communications security, system development, management and maintenance, and system security.

National Guidelines

These have been issued to assist AFP employees to observe the policies and standards in the following relevant areas:

- Electronic Mail
- Financial Statements
- Home based work - security
- Identity Certificates
- Information Release pursuant to Freedom of Information Act 1982
- Internet
- Intraweb Publishing
- Security Access Control
- Security Plan
- Voice Mail
- Work at home (occasional) – security.

Yours sincerely

C.J.Whyte
General Manager
Policy & Commercial