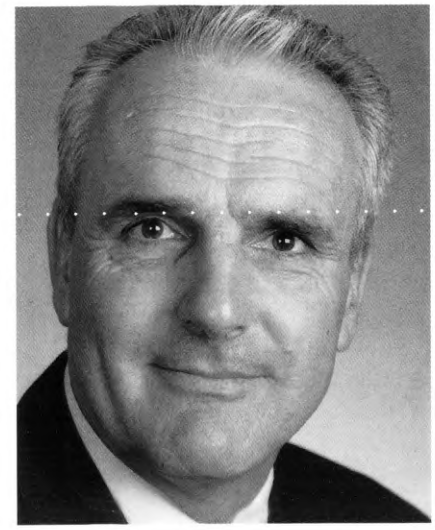
The AFP and Commonwealth department security management

By Phil Baer
General Manager Eastern Region

In addressing an audience of Commonwealth department internal security personnel, General Manager of AFP's Eastern Region, Phil Baer outlined the implications of the introduction of the Commonwealth Fraud Control Policy and the effect on the application of this policy brought about by recent and ongoing changes to the role, function and structure of the AFP.

The audience represented the range of federal government departments that require internal security strategies. Mr Baer sought to inform the departmental representatives on how to best factor the AFP into departmental security management.

He touched on some of the constraints facing the AFP and discussed the impact of the Commonwealth Fraud Control Policy.



Phil Baer
General Manager Eastern Region

To cope with a diminished resource base, the AFP now operates a national system for ranking incoming tasks before making a determination to accept or reject that task. The priority system addresses many issues, with the two major ones being an impact assessment and a resource intensiveness assessment.

Monetary value is only one factor in determining impact. Some departments have expressed dissatisfaction with the concept of a priority model, given that some referrals do not attain sufficient priority to be accepted for investigation. Setting priorities for referrals, however, is in accordance with published government policy.

Government has properly decreed that the AFP, more often than not, in a strategic alliance with the National Crime Authority (NCA) and/or our other Australian and international law-enforcement partners, will concentrate on those criminal activities which most impact on Australia. The security of government programs is an obvious priority, although, in the first instance, not a police responsibility but rather the responsibility of the chief executive officer of the respective departments and agencies.

When discussing security in Government it is necessary not only to consider the Protective Security Manual but also the impact of the Fraud Control Policy. There is considerable commonality between the requirements of the two. This commonality extends to staff vetting, physical protection which includes building access controls, procedures for securing information, computer

and communications security standards. It is arguable that not only should there be a close liaison between the areas responsible for the requirements of each but that one area should be responsible for both, such is the degree of commonality.

The issue of the Fraud Control Policy in 1994 created new responsibilities both for the AFP and for departments and agencies. The policy has expanded the role and responsibilities of the AFP in respect of security management as it relates to fraud.

The AFP is, pursuant to the Fraud Control Policy, tasked with maintaining a Commonwealth Fraud Information Database (CFID). All departments and agencies are required to contribute to CFID and to, at least quarterly, update their contributions until such time as the matter is finalised.

Pursuant to the Fraud Control Policy, financial impact statements relative to new policy proposals must now include estimates relating to fraud and the costs on the criminal justice system, as well as a criminal damage risk assessment.

The AFP, in conjunction with the Commonwealth Law Enforcement Board (CLEB), Australian National Audit Office (ANAO) and the relevant agency, now has a role in advising Government as to how well an agency meets the standards set for fraud control. In respect of agency fraud investigation units the AFP has a role to work with those units to establish best practice investigation procedures.

The AFP, during the first half of 1996 will commence an annual program of quality assurance reviews of agency investigations as required by the Fraud Control Policy. The AFP has been given the role of delivering fraud investigation and relative training. It is incumbent upon all agencies to ensure that all personnel investigating fraud against the Commonwealth receive training either from the AFP or internally, where an internal course has been approved by CLEB.

The AFP is obliged to inform an agency within 28 days of either the acceptance or rejection of a referral and, in the case of an acceptance, the name of the investigating member. The AFP is also obliged to provide agencies with quarterly case management reports where AFP action is outstanding.

Thus it can been seen that the Fraud Control Policy has many implications for departments and agencies as well as the AFP. Many of these implications for departments and agencies have a security management aspect. Obviously the Fraud Control Policy has been responsible for changes within the AFP. However, it has not been the sole influence.

Changes to the AFP

The AFP today is a vastly different AFP to that which existed as little as 12 months ago. Today, the AFP actively seeks to promote strategic alliances with our law-enforcement partners be they agency, state, national or international in dimension. Where there is a law-enforcement benefit, the AFP responds favourably to requests for the outposting of its members to agencies. The AFP seeks to be involved in day-to-day co-operative investigation arrangements and bilateral and multilateral operations of either a local, national or international character.

The AFP can provide assistance to agencies in fields such as training, computer-crime investigation, the application of forensic sciences, particularly document examination including handwriting analysis, as well as crime scene recording and evidence preservation. As the CFID develops, the AFP will be able to assist agencies in regard to trend analyses.

By far the greater majority of department and agency security-related matters coming to AFP notice involve some act of commission or omission by staff of that department or agency. In saying this, I include the AFP.

The AFP also is undergoing rapid change. The major thrust of the change is to provide an organisation which comprises empowered customer-focused teams which form, and reform, according to the task at hand and the mix of skills needed to best deal with that task. This has seen a further move away from the traditional hierarchical (militaristic) and heavily prescriptive structure that has hitherto characterised police organisations. These changes are continuing to this date.

It has been, and continues to be, the AFP experience that the greatest risk to [an organisation's] security lies with its own people. By far the greater majority of department and agency security-related matters coming to AFP notice involve some act of commission or omission by staff of that department or agency. In saying this I include the AFP.

Security vetting prior to appointment offers no guarantee that those who satisfy the checks are going to perform to the desired standard of integrity and honesty throughout the length of

their employment. This highlights the need for some form of ongoing integrity checking of those in key positions or with access to sensitive data.

The advent of widespread computer use and increasing levels of computer literacy within the Commonwealth's workforce, and in the community generally, raises several problems for security managers.

With the increasing levels of computer skills in our society it becomes increasingly difficult to state that any particular means of identification can be relied upon.

To date the AFP has been involved in a number of cases involving the unauthorised copying of data, the selling of data after accessing it on a computer system, the falsification of data and the erasure of data, all by Commonwealth employees. In another instance a programming contractor altered one of a department's computer programs to automatically transfer funds to an individual's bank account.

Counterfeiting

The Commonwealth also has been the victim of non-Commonwealth employees who have used their computer skills to produce counterfeit documents ranging from identification papers such as birth certificates to high quality forged bank notes. In one instance, federal agents recovered what amounted to the results of very detailed research into scanner, printer, software and computer combinations to determine which one combination was best to produce quality forged banknotes. The research was thorough and the results well recorded. The resultant forged banknotes were also of a good quality.

With the increasing levels of computer skills in our society it becomes increasingly difficult to state that any particular means of identification can be relied upon. The AFP has seen forgeries in passport, citizenship papers, marriage certificates, death certificates, birth certificates, drivers' licences, credit cards, telephone cards – the list goes on. There is little that is immune from a person with access to a reasonable level of computer skills and technology.

The technological battle to produce documents incapable of being readily and unlawfully reproduced at a good standard is one which can never end. Australia's polymer bank notes are a good example of forgery-resistant documents. However, I have no doubt that forgers are already turning their minds to defeating even these. The Australian passport, while relatively difficult to forge, is easily obtained using false identification and certification. Thus the technology underlying the production of the passport is beaten by corruption of the system at the application level.

As departments and agencies alter the way they do business, old vulnerabilities vanish and new opportunities are created. As more and more computer systems are linked in the normal course of business and as such links extend to external organisations, the opportunity for computer crime increases.

Computer crime

The AFP treats offences which fall within Parts VI A and VII B of the *Crimes Act 1914* as being computer crime. (The equivalent NSW state offences for computers are to be found at Part 6, ss.308-310, *Crimes Act 1900*.)

Briefly, Part VI A deals with computer systems while Part VII B deals with telecommunications networks. The AFP approach recognises that technology has progressed to the point where our telephone networks and PABX equipment are computer controlled. The major difference between these manifestations of information technology is in the user interface.

The initial problem confronting police is to determine if there is a criminal offence. There are basically three issues:

- intentional and unauthorised access to data
- persistence in unauthorised access with aggravating circumstances
- tampering with data.

Maximum penalties for Commonwealth offences range from six months imprisonment through two years to 10 years. Commonwealth legislation makes no specific provision for copying or extracting data. This issue is one of many being addressed in a law reform paper being prepared by the NCA. It is also very relevant to organisations dealing with foreign governments and companies, particularly in the trade arena.

Much of the information used in such dealings will be commercially sensitive and unauthorised disclosure has the potential to significantly affect Australia's trade relations and balance of payments.

Whenever a computer security manager has reason to believe that there has been an attack on, or unauthorised access to, a computer system I implore them to immediately contact the AFP co-ordination centre at the regional head office in their capital city.

While, understandably, a security manager will want to plug the breach immediately, this may well destroy vital evidence or deny the opportunity for the AFP to deploy specialised equipment to identify the offender. The need to prevent further

breaches of security and the police desire to preserve evidence to identify the offender and bring the offender to justice need not be mutually exclusive provided early consultation takes place. It should be borne in mind, just closing the door on a detected unauthorised access is not enough. The crime must be reported because an intruder, having once gained unauthorised access to a system will almost certainly try again.

It is difficult to quantify the extent of computer crime in Australia. Anecdotally we are led to believe that only a very small percentage of such crimes is reported. The usual explanation being the fear of creating a lack of confidence in an organisation or its management. I have no reason to suspect that this is the case in Commonwealth departments and agencies. Despite the lack of confidence in reporting statistics the AFP does receive sufficient reports of computer crime from private organisations to justify a belief that the problem of computer abuse in Australia is a significant one.

Our experience to date shows that the most likely offender is not the analyst or IT manager but the end user, disgruntled former employee and hacker or cracker. All computer systems are open to abuse and the first step in protecting them is a thorough risk analysis. The AFP may be able to assist in this regard through a knowledge of attacks on other systems within Australia and lessons learnt from investigating them. In the final analysis there has to be a trade-off between putting computers to use and securing them from misuse or abuse. The role of good housekeeping, including security audit trails, cannot be too strongly emphasised as the first proactive deterrent to security breaches. Targeted and random security audits are essential elements of this housekeeping.

From a law-enforcement perspective, I cannot stress too strongly the value of a documented information technology security policy which has been approved at the highest level. This document should be readily available to all staff and it should unambiguously set out what their information technology roles and responsibilities are. This document is the starting point in internal matters in proving that someone knew what they were doing was wrong.

The investigation of computer security breaches, where a criminal offence is alleged, will more often than not require a joint effort between IT people and AFP investigators. While the AFP maintains, in the larger regions, experienced core computer crime teams, they will still require the expert technical assistance of an organisation's own personnel. In many instances this will involve your expert being a potential witness for the prosecution.

The problems of detection are not insurmountable and importantly, are not the problem of IT security personnel and police alone. End users must be educated in the need for, and the benefits of security. Their active participation must be sought. They must be encouraged to look for and report any anomalies or suspicions. Prevention is better than cure and to that end the AFP is happy to provide expert speakers on the subject of computer crime if departments and agencies request it.

If issues are clouded and complicated now, the future is even more unclear. As information technology develops, traditional demarcations between voice, text and images are disappearing. All are increasingly processed and transmitted as binary data, and distinctions between computer, public switched telephone network, private automatic branch exchanges and picture/film/recording libraries become blurred or even meaningless.

Many people now have an appreciation, and experience, of a local area network (LAN). Some may even understand the workings of a wide area network (WAN). Businesses and governments use this technology to allow decentralisation, provide better communication and co-operation between offices and usually expect an increase in productivity.

Despite the lack of confidence in reporting statistics, the AFP does receive sufficient reports of computer crime from private organisations to justify a belief that the problem of computer abuse in Australia is a significant one.

In one sense it recognises the fact that we tend to work in groups rather than as individuals, particularly when the work becomes more complicated. School children are being introduced to the Internet. What was once considered the preserve of a few has suddenly become available to many.

Just as the size of networks is increasing, so too is the number of service providers. These organisations are driven fundamentally by marketing issues and staff in them may not necessarily share the same views about network security. The basic issue for them is to provide a successful connection from A to B, rather than worry about the legality of the connection at B.

The past few years have seen a rapid increase in the use of networks and the trend is likely to

continue unabated. We are forever demanding more and better information and we want it now! This pressure will almost certainly lead to increased use of:

- dedicated networks;
- packet networks provided by third parties, and
- the global network known as the Internet.

This increased connectivity usually has quite demonstrable benefits however we should not lose sight of the dangers inherent in its adoption. Firstly, there is lack of control through the involvement of other enterprises: on September 20, 1995, twenty Commonwealth government departments, 28 agencies and six parliamentary departments maintained a presence on the Internet. We are increasingly forced to rely on security systems and the integrity and dedication of our people for the protection of our data.

Increasingly, the requirement is to use common systems to process and communicate information, with inputs and outputs being in whatever combination of human audio/visual sensory perception best suits the purpose. In this complex social and economic environment it is unrealistic to expect any law-enforcement agency to carry the fight for security and data integrity. Whatever progress we make can only be sustained through co-operation.

As security managers, you need to ensure that computer systems are resistant to attack and, in a worst-case scenario, provide an uncorrupted audit trail. After all, theft now is not constrained by the limits of the human body — it can take place across national and international borders with ease, commonly occur at 10 megabits/second or better, and in the absence of an effective audit trail, remain virtually undetected. In such an environment, the primary responsibility for ensuring security and privacy of corporate data lies with departmental and agency security managers.

It should be recognised by everyone that computer-related crime not only has an economic character but other serious consequences for the human race. Society relies on computerised systems for almost everything in life, from air traffic control, the regulation of trains and traffic, medical services or national security. Effective counter measures, regulation and enforcement are essential for the continuing prosperity and well-being of the Australian community.

The AFP of today is about co-operative law-enforcement efforts, partnerships, strategic alliances and the provision of a quality law-enforcement service to the people of Australia. Our vision is to fight crime and win. □

Mr Baer thanked Federal Agent Chris Buttner, Core Computer Crime Team, Eastern Region for his assistance in developing a draft paper which provided the genesis for the computer crime material in this paper.

Commonwealth fraud control policy

The Commonwealth Fraud Control Policy places obligations on the AFP and on Commonwealth agencies and departments. The policy states that fraud of a minor or routine nature should be investigated by those agencies being affected, while serious criminal offences should be handled by the AFP.

Although the policy does not define "serious criminal offences", it does require the AFP "to conduct all investigations directed towards *Crimes Act 1914* prosecutions", subject to three exceptions:

- agencies which prosecute fraud cases under their own legislation should continue to investigate matters where the *Crimes Act* is considered more appropriate and the DPP is satisfied that the prosecution brief does not require AFP involvement;
- agencies which can satisfy both the AFP and the DPP that they have the capacity and capability to investigate criminal cases; and
- matters involving multi-jurisdictional organised crime are referred to the NCA.

The AFP, however, still retains the discretion to make arrangements with particular agencies regarding the investigation of certain minor fraud matters, especially where an agency does not have its own investigative capacity.

To ensure investigations are proceeding effectively, regular meetings are held between the AFP and agencies conducting investigations. Meetings are conducted throughout Australia and liaison officers have been appointed to review progress of fraud investigations within their particular region.

Under the new fraud-liaison arrangements, the AFP is required to implement a 28-day turnaround on the acceptance or rejection of referrals from Commonwealth agencies and to provide quarterly reports to client agencies on significant developments in investigations as well as status reports on the progress or outcomes of investigations that have been referred to the AFP.

Relevant operational areas prepare quarterly case management reports which cover all cases of crime referred to the AFP:

- where the alleged criminal conduct has been perpetrated against a Commonwealth agency, against programs administered by it, or against legislation for which the agency has responsibility;
- which have been referred to the AFP and accepted for investigation by the relevant operational area; and
- which have either not been finalised or have been finalised in the current reporting quarter.

To minimise large peaks in workload, the preparation of reports has been staggered, the first quarterly reports to three agencies were delivered on August 11, 1995. Commissioner Palmer has emphasised the need for co-operation and understanding between Commonwealth agencies and the AFP. He said AFP senior management was ready to assist in clarifying the AFP's investigational role and discuss any concerns that Commonwealth agencies might have.