CCC EXHIBIT

PROTECTING CONFIDENTIAL INFORMATION

A REPORT ON THE IMPROPER ACCESS TO,
AND RELEASE OF,
CONFIDENTIAL INFORMATION FROM THE POLICE
COMPUTER SYSTEMS BY MEMBERS OF THE
QUEENSLAND POLICE SERVICE

NOVEMBER 2000

QUEENSLAND
CRIMINAL
JUSTICE
COMMISSION

CCC EXHIBIT

CCC EXHIBIT

FOREWORD

This report presents the results of a review, undertaken by the Criminal Justice Commission (CJC), of the information-security policies, procedures and practices of the Queensland Police Service (QPS). The report puts forward a comprehensive set of recommendations, which, if implemented, should substantially reduce the risk of police officers and other QPS employees improperly accessing and releasing confidential information held in the police computer systems.

The review was prompted by a CJC investigation, initiated in August 1998, into allegations that police officers stationed at the Nerang Police Station may have been unlawfully disclosing confidential government information from the QPS computer systems to a cleaner who was employed at that station. Initial investigations suggested that the allegations had substance and that the suspected misconduct was widespread.

During the course of the investigation, the CJC received other allegations of police officers unlawfully disseminating QPS information. In addition, there was a steady flow of similar complaints that could not be productively investigated because of issues relating to current QPS information systems. In order to investigate those matters that the CJC could pursue, it was decided to commence an inquiry known as Project Piper.

In December 1999 the Commission resolved to conduct hearings into the alleged improper access to, and release of, confidential information from the police computer systems by members of the QPS. At the conclusion of this investigative phase of the Inquiry, the CJC heard submissions from interested stakeholders over three days of public discussion in order to ensure that all issues were considered from a number of perspectives.

The evidence that the hearings and the submissions disclosed led the CJC to take a proactive approach aimed at reducing the future incidence of improper access to, and/or release of, confidential information. This process was undertaken with the support of the Commissioner of Police, who acknowledged the challenges posed by technological developments in recent years. On this, as for other issues, the CJC has sought to work with the QPS in the shared objective of continuing the reform process.

The report has required a balancing of many difficult and important issues and concerns. However, we are satisfied that the recommendations made in it are workable, while providing for a proper level of accountability. As is standard practice, there has been extensive consultation with the QPS in the finalisation of the report.

Although the report draws attention to deficiencies in the QPS systems for managing information security, it should be recognised that major gains have been made by the QPS over the last decade in raising levels of integrity within the Service and reducing the opportunities for misconduct. With respect to the specific area of information security, the QPS has developed an information-security policy-development framework that has resulted in comprehensive policies and procedures to reduce the risk of breaches of information security. The Service has also developed a comprehensive computerised information system that includes a facility to examine any transactions conducted by computer users. More generally, significant steps have been taken to build up an 'integrity framework' within the Service as a whole, as evidenced by such initiatives as the establishment of the Ethical Standards Command. The recommendations made in this report represent a collection of complementary changes and initiatives that will further reduce the risk of misconduct within the Service.

It should be acknowledged that the problems that have been identified in relation to

CCC EXHIBIT

CCC EXHIBIT

QPS systems and processes are not unique to the QPS but, rather, are characteristic of large police organisations in general, and most likely of many other non-policing bodies. However, the fact that the problems are not restricted to the QPS is not, of course, a justification for inaction or delay in addressing these problems.

The report is primarily concerned with the QPS but it will be of interest to all areas of government because a wider range of information is increasingly available to public-sector employees. It is important that agencies and departments take a strategic and proactive stance in the development of information-security systems. To do otherwise may result in embarrassing and costly breaches of information security.

As is standard practice for inquiries of this nature, the CJC will monitor the implementation of recommendations made in this report and may make a further report to Parliament, if this is considered necessary.

Brendan Butler SC
Chairperson
Criminal Justice Commission

CCC EXHIBIT

CCC EXHIBIT

RECOMMENDATION 6.9 — TECHNOLOGY FOR INFORMATION SECURITY **P. 64**

6.9.1 That, as a matter of priority, the Queensland Police Service progressively incorporate information-technology capabilities within the next three years to:
- install an 'alert' monitoring feature for selected records and transactions
- install a 'barring-access' function for selected records and information
- develop and implement a system for detecting excessive transactions by authorised users.

6.9.2 That, as part of strategic planning, the Queensland Police Service continues to monitor the development of new IT capabilities that can assist in the protection of information and the detection of inappropriate use.

RECOMMENDATION 6.10 — SYSTEMATIC AND ONGOING INTERNAL AUDIT **P. 66**

6.10.1 That the Queensland Police Service give higher priority to the use of audit strategies to prevent this type of misconduct by developing and implementing a systematic and ongoing internal audit program, which is both random and targeted, of access to and use of the computer corporate/mainframe systems.

6.10.2 That, as part of the risk-management process, managers and supervisors incorporate a program of local internal audit of access to and use of computer corporate/mainframe systems.

RECOMMENDATION 6.11 — REASON FOR TRANSACTION **P. 71**

6.11.1 That the Queensland Police Service order that all members must record a reason for access for each transaction made on the corporate/mainframe computer systems, either through mandatory computer entry, police notebook entry, or some other systematic documentation process, except where:
- a series of transactions are logically linked, in which case a single reason for the multiple transactions will afford an appropriate level of accountability
- where other official police documents provide evidence of an appropriate reason for the transaction
- where the duties of an officer require an unusually high number of transactions in relation to information that would routinely be accessed (e.g. a traffic police officer performing vehicle registration checks).

The last proviso should not apply to those members accessing sensitive information, such as intelligence databases.

6.11.2 That, where transactions are conducted on behalf of another member, the requesting member be required to record a reason for the request through mandatory computer entry, police notebook entry, or some other systematic documentation process.

6.11.3 That, where transactions are performed on behalf of another member, the person conducting the transaction asks the requesting member the reason for their request and their name, and records that information through mandatory computer entry, police notebook entry, or some other systematic documentation process.

RECOMMENDATION 6.12 — RAISING AWARENESS OF INFORMATION SECURITY AND INDIVIDUAL ACCOUNTABILITY **P. 74**

6.12.1 That, in response to this report, the Commissioner of Police issue a notice to all members, addressing the issues arising from this Inquiry, areas of concern and policy developments in respect of information security.

CCC EXHIBIT

6.12.2 That the Queensland Police Service require all members to sign an acknowledgment stating that they:
- agree to the information-security policies as specified
- fully understand that the QPS computer system is not for personal use and therefore should only ever be accessed and used in the performance of official police work
- have read the legislation and will abide by the legislation, orders, policy and procedural rules and guidelines on computer use and access, and release of information
- understand that a breach of the terms of the contract/agreement will result in criminal and/or disciplinary action and possibly dismissal.

To ensure that no significant administrative burden is placed on the QPS, implementation should be progressive and be applicable to all new recruits from January 2001.

6.12.3 That a supervisor or manager witness the signing of the acknowledgment, and also attest that the member has demonstrated that he/she has read the contract/agreement and fully understands its content.

6.12.4 That, where a supervisor or manager is not satisfied that a member has the necessary understanding of legislation, orders, policies and procedures relating to security of computer information, access should not be granted until the member completes appropriate training and education

6.12.5 That all members be required to re-sign their acknowledgment when they request new, changed or renewed access to a mainframe/corporate system or database

---

RECOMMENDATION 6.13 — EXTENDING INFORMATION SECURITY **P. 76**

6.13.1 That the Queensland Police Service incorporate, in higher education and training programs, particularly those catering for supervisors and managers, training sessions/modules on computer use, information security, and supervision of computer use by subordinates.

6.13.2 That the Queensland Police Service educate managers and supervisors on the application of the principles of risk management to develop processes for the effective monitoring and supervision of subordinate staff in the use of and access to the police computer system.

6.13.3 That the Queensland Police Service complete the development of the Competency Acquisition Program module on computer use and information security.

RECOMMENDATION 7.1 — ACCESS TO CRIMINAL HISTORY, DRIVER'S-LICENCE AND VEHICLE-REGISTRATION RECORDS **P. 90**

That the Government should review the restrictions that currently apply to accessing criminal histories, and driver's licence and vehicle-registration particulars, to determine whether any of those restrictions can be varied or waived in certain cases.

CCC EXHIBIT

1 INTRODUCTION

The protection of confidential and personal information collected by government agencies and departments has emerged as an important and often controversial issue, both nationally and internationally. Within Australia, numerous agencies and groups have expressed their interest in this issue by way of investigative and/or public reports, media articles and reports, and other documents such as the Australian and New Zealand Standard on Information Security Management (AS/NZS4444.1:1999, AS/NZS 4444.2:1999). This is also an area of increasing community concern, as it is often the personal and private details of community members that are at risk.

As new information system technologies and initiatives are adopted in the public sector, a growing number of public servants have acquired the capacity to access the massive amounts of confidential information available on integrated computer systems. Such advances greatly assist government departments and agencies in the delivery of services to the community, and in making their internal operation more efficient. However, with these advances come new and emerging risks. It is important that these risks are effectively managed and that appropriate risk-reduction strategies are adopted to minimise the chance of confidential information being misused.

This chapter begins with a description of the scope of the report. This is followed by a section outlining the statutory powers and responsibilities of the CJC to investigate and report on 'misconduct' and 'official misconduct', and to provide advice and/or assistance to law-enforcement agencies on the detection and prevention of official misconduct. The next section describes the genesis of this investigation and the background leading to the Public Inquiry. The final section sets out the structure of the report.

SCOPE OF REPORT

This report has resulted from the CJC's Inquiry into alleged improper access to, and release of, confidential and personal information from the police computer systems by members of the Queensland Police Service (QPS).

The aim of the report was to examine and suggest remedies for the issues of concern relating to this type of misconduct, as revealed during this and previous investigations. It is essentially a report focusing on methods of risk-reduction and risk-prevention rather than a report of the investigative findings of this Inquiry.

The CJC's objective was to develop recommendations aimed at:

- reducing the incidence of misconduct of this nature within the QPS
- modifying QPS information-management systems to improve information security and afford greater protection to information that is accessible through the corporate/mainframe computer systems
- ensuring that the personal and confidential information is given an appropriate level of protection through legislation.

To achieve this objective, the CJC was required to review, in detail, the current policies, procedures and practices of the QPS with regard to information-security management. This was a significant undertaking given that the QPS has been very active in this area (detailed in chapter 5). The purpose of this review was to identify the measures taken by the QPS to preserve information security and, by identifying any 'gaps' within the framework of its information-security management, to assist in further reducing the opportunity for this misconduct to occur.

The report is not only concerned with information-security management within the QPS; it also considers the nature of the market for information and examines current government provisions for the release of restricted

CCC EXHIBIT

CCC EXHIBIT

attempting access. This would act as another system for monitoring and detection.

The South Australia Police use bars on records that relate to sensitive murders and rape-victim details. The identity of people who attempt to access barred information is recorded, and they are asked to explain.

3. 'Alert' system for excessive transactions — This is a simple 'alert' system that can be extremely useful in monitoring computer systems for excessive levels of access. Some concern was raised that this type of alert system may result in busy officers being unfairly targeted for audit and investigation. However, the use of benchmarks and the implementation of a properly instituted system of 'alert' monitoring for excessive transactions, together with a clear understanding of the need for accountability, would counteract this tendency.

An effective system would have different thresholds for different classes of employees. For example, traffic officers would have a significantly higher threshold for access to vehicle-registration information than the typical general duties police officer.

In most cases any investigation would begin by approaching the subject officer's supervisor, who may be able to justify the level of computer inquiries, thereby obviating the need for any further investigation.

It is important that the QPS continue to be vigilant in assessing and considering new IT measures to assist in the protection of information and the detection of inappropriate use through the strategic planning process. As IT innovations emerge, there will be a corresponding need for the development of appropriate and effective control mechanisms.

RECOMMENDATION 6.9 — TECHNOLOGY FOR INFORMATION SECURITY

6.9.1 That, as a matter of priority, the Queensland Police Service progressively incorporates information-technology capabilities within the next three years to:

- install an 'alert' monitoring feature for selected records and transactions
- install a 'barring access' function for selected records and information
- develop and implement a system for detecting excessive transactions by authorised users.

6.9.2 That, as part of strategic planning, the Queensland Police Service continues to monitor the development of new IT capabilities that can assist in the protection of information and the detection of inappropriate use.

SYSTEMATIC AND ONGOING INTERNAL AUDIT

It is well documented within corruption-prevention literature that internal audit is an effective deterrent and detection mechanism. Certainly users are more likely to be tempted to misuse the computer system if they believe there is little chance that they will be detected.

The CJC regularly surveys FYCs (First Year Constables) concerning their views on ethical conduct and the disciplinary and complaints process. Respondents are presented with 10 scenarios illustrating various forms of unethical conduct and asked several questions about the scenarios, including 'How would you rate the likelihood of an officer who engaged in such behaviour being caught?'. The scenarios are shown in table 6.2.

Data collected before this Inquiry began demonstrate that junior police officers believe it is unlikely that an officer would be 'caught' for conducting a vehicle-registration check to obtain the address of an attractive women seen driving a car (scenario 7). As shown in figure 6.2, FYCs rate the likelihood of being detected for improper computer access as described in scenario 7 as unlikely.

The views of the FYCs are probably correct, given the evidence gathered during this Inquiry. This perception was confirmed by one subject police officer:

> Chairman: So although that screen [referring to computer warning screen] tells you that the checks can be audited, at the time you made these checks you didn't really think that there was much chance of anyone picking it up?
>
> NQ1: It would have been safe to say it, yeah. (CJC unpub., p. 633)

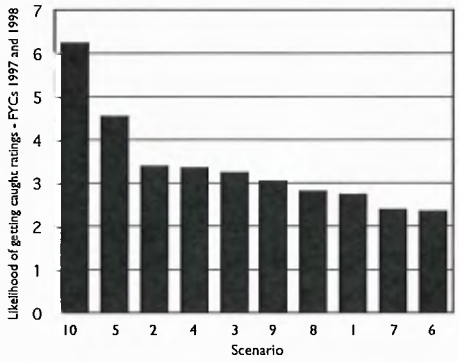
In its submission (pp. 48–49), the QPS stated that auditing is used, but there is no systematic and ongoing program of audit specifically for computer access.

CCC EXHIBIT

Table 6.2 — Scenarios in the CJC survey on ethical conduct

Scenario 1	Off-duty officer tried to avoid Random Breath Test
Scenario 2	Officer at bottle shop break-in pockets cigarettes
Scenario 3	Officer retaliates against youth who assaulted female officer
Scenario 4	Accident by police misrepresented in report
Scenario 5	Words added to suspected rapist's statement
Scenario 6	Pick-up of personal items outside of patrol area
Scenario 7	Registration check to get details of an attractive woman
Scenario 8	Officers accept cartons of beer for Christmas party
Scenario 9	Officer forcibly moves youth on
Scenario 10	Officer engages in 'skimming' from drug exhibits

Figure 6.2 — Perceived likelihood of being detected for improper and unethical conduct



Source: Research and Prevention Division, CJC

Notes:
1. Rating scale is 1 to 7, with 1 being 'not at all likely' and 7 being 'very likely'.
2. Subjects were First Year Constables surveyed in 1997 and 1998.
3. N size for each scenario ranged from 263 to 268.
4. A brief description of each scenario is given above.

It is well documented that best practice in information security is characterised by follow-through compliance checking, with the policies and procedures in place. As the Office of the NSW Ombudsman commented in their written submission (2000, p. 20):

> 83. For officers intent on improperly accessing information, the most powerful disincentive is the prospect of being found out. This is only likely to occur if such officers are aware that frequent random audits are occurring.
>
> 84. Given the harm that may arise from improper accesses, it is important that audits be conducted frequently to maximise the likelihood that improper accesses are detected early.

As the Inquiry heard, other jurisdictions have commenced systematic internal audit programs for computer use:

- **NSW Police Service** — With the introduction of a new computer system in 1994, the NSW Police Service commenced a systematic random audit program of accesses made to the system. The auditing processes are conducted at two levels: the Audit and Evaluation and Internal Affairs conduct targeted and random audits, whereas Commanders/Managers perform quarterly checks of 25 per cent of personnel and their computer accesses. All staff are audited annually. The NSW Police Service also uses IT initiatives to assist in the audit process. Special audit software continuously monitors the systems to detect any attempts at improper accesses.

  The Office of the NSW Ombudsman reported that the commencement of the random audit of computer accesses resulted in an increased number of internal police complaints. This indicates that there are clear benefits in having an internal audit program on computer access. The NSW Police Service reported at the Inquiry that 27 police (serving and former) had been charged either criminally or by summons for a total of 147 offences relating to 'unlawful access to computer'. As a long-term consequence of information-security initiatives, the NSW Police Service reports that the rate of complaints about the provision of unauthorised information and misuse of the computer system is now declining.

CCC EXHIBIT

- **SAPOL (South Australia Police)** — A member of Information Systems and Technology Service is the designated data-integrity and security-systems officer, who conducts about 200 separate audits per year. These include audits on the accessing of records of high-profile individuals who have appeared in the media. SAPOL is also moving toward giving some audit responsibility to divisional managers.
- **VICPOL (Victoria Police)** — VICPOL conducts both random and targeted auditing of computer access to the Law Enforcement Assistance Program (LEAP), which is conducted by both the LEAP project office and an internal audit team.

The individuals representing each jurisdiction reported positive results from implementing internal-audit processes. Some of the above programs are random, meaning that all members have an equal probability of being selected for an audit. Other programs are targeted, for example the one used by SAPOL, which involves checking accesses to the records of high-profile individuals. Both types of audit, random and internal, are useful for detecting improper access to confidential information held on the computer systems.

Random audits provide a powerful deterrent effect, as has been observed in the literature on the use of random breath-testing. Targeted audits are extremely useful in high-risk areas. The technological functions recommended above will greatly enhance the ability of the QPS to conduct effective targeted audits.

This is an opportune time for the QPS to make a commitment to introduce a program of systematic and ongoing internal audits. The program should have both random and targeted components. The issue of how to design such a program is a matter for the QPS.

To promote greater area/unit responsibility, local areas should incorporate within their risk-management processes a system of local internal audits of access and use of QPS computer corporate/mainframe systems. The provisions for this are set out in chapter 15 ('Risk-Based Assessment System') of the OPM

RECOMMENDATION 6.10 — SYSTEMATIC AND ONGOING INTERNAL AUDIT

6.10.1 That the Queensland Police Service give higher priority to the use of audit strategies to prevent this type of misconduct by developing and implementing a systematic and ongoing internal audit program, which is both random and targeted, of access to and use of the computer corporate/mainframe systems.

6.10.2 That, as part of the risk-management process, managers and supervisors incorporate a program of local internal audit of access and use of computer corporate/mainframe systems.

'REASON FOR TRANSACTION' REQUIREMENT

During the course of this investigation and similar inquiries elsewhere, many officers claimed to have no recollection of the computer inquiry in question or the reason why it was conducted. In the case of the Nerang Police Station, the CJC was only able to go behind this response because it had conducted an extensive investigation with the benefit of documentation that it obtained by means of a search warrant. This is not always possible.

In the absence of any other means by which to prove or disprove whether access was appropriate, an investigator must accept the 'can't recall' defence. Similarly, audits of computer access can only be conducted effectively if users are required to demonstrate why they accessed the computer systems.

The New South Wales experience on reason for transaction

The NSW Police Service is the only jurisdiction to implement a mandatory recording of reason for transaction Service-wide. There are some parallels between the development of that system and the history of this debate in Queensland.

In 1992, the ICAC released a report on an investigation of improper access and release of confidential government information. The investigation revealed a highly active illicit information trade that involved public servants from various government departments and agencies, including the NSW Police Service. It revealed the inadequacies of information-security management in many departments and agencies.

In May 1993, the NSW Ombudsman released a provisional report on one matter of this nature (Office of the NSW Ombudsman 1994). It was recommended that, to solve these problems, the NSW Police Service insert a 'reason for transaction' field that users would have to complete before they could obtain access to the computer system. The NSW Police Service rejected the recommendation because:

- the insertion of such a field would generate costly overheads

CCC EXHIBIT

CCC EXHIBIT

1 INTRODUCTION

The protection of confidential and personal information collected by government agencies and departments has emerged as an important and often controversial issue, both nationally and internationally. Within Australia, numerous agencies and groups have expressed their interest in this issue by way of investigative and/or public reports, media articles and reports, and other documents such as the Australian and New Zealand Standard on Information Security Management (AS/NZS4444.1:1999, AS/NZS 4444.2:1999). This is also an area of increasing community concern, as it is often the personal and private details of community members that are at risk.

As new information system technologies and initiatives are adopted in the public sector, a growing number of public servants have acquired the capacity to access the massive amounts of confidential information available on integrated computer systems. Such advances greatly assist government departments and agencies in the delivery of services to the community, and in making their internal operation more efficient. However, with these advances come new and emerging risks. It is important that these risks are effectively managed and that appropriate risk-reduction strategies are adopted to minimise the chance of confidential information being misused.

This chapter begins with a description of the scope of the report. This is followed by a section outlining the statutory powers and responsibilities of the CJC to investigate and report on 'misconduct' and 'official misconduct', and to provide advice and/or assistance to law-enforcement agencies on the detection and prevention of official misconduct. The next section describes the genesis of this investigation and the background leading to the Public Inquiry. The final section sets out the structure of the report.

SCOPE OF REPORT

This report has resulted from the CJC's Inquiry into alleged improper access to, and release of, confidential and personal information from the police computer systems by members of the Queensland Police Service (QPS).

The aim of the report was to examine and suggest remedies for the issues of concern relating to this type of misconduct, as revealed during this and previous investigations. It is essentially a report focusing on methods of risk-reduction and risk-prevention rather than a report of the investigative findings of this Inquiry.

The CJC's objective was to develop recommendations aimed at:

- reducing the incidence of misconduct of this nature within the QPS
- modifying QPS information-management systems to improve information security and afford greater protection to information that is accessible through the corporate/mainframe computer systems
- ensuring that the personal and confidential information is given an appropriate level of protection through legislation.

To achieve this objective, the CJC was required to review, in detail, the current policies, procedures and practices of the QPS with regard to information-security management. This was a significant undertaking given that the QPS has been very active in this area (detailed in chapter 5). The purpose of this review was to identify the measures taken by the QPS to preserve information security and, by identifying any 'gaps' within the framework of its information-security management, to assist in further reducing the opportunity for this misconduct to occur.

The report is not only concerned with information-security management within the QPS; it also considers the nature of the market for information and examines current government provisions for the release of restricted

CCC EXHIBIT

CCC EXHIBIT

user enters the system. However, there are arguably better strategies, such as those recommended throughout this report, to raise the general awareness of the user.

The QPS currently requires civilian members to sign a confidentiality agreement in relation to computer access and use (see page 51) before being permitted to begin using the computer system. This agreement is similar to the Statement of Responsibility (figure 6.4), which all members of the NSW Police Service are required to sign at the commencement of their employment.

The CJC considers that it should be compulsory for all members of the QPS to agree to and sign a confidentiality acknowledgment. The purpose of the acknowledgment is to raise awareness, improve accountability and emphasise the importance of information security. The acknowledgment makes users responsible for transactions made under their user-ID and places the onus on them to demonstrate that their transactions were for official police work.

As part of a strategy to emphasise individual responsibility and accountability in the use of the computer system, all members of the QPS should be required to sign an acknowledgment that they:

- agree to the information-security policies (e.g. 'Never disclose your password', 'Never leave an open terminal unattended', 'Always record a reason for transaction except where exemptions are made under QPS policy') that are listed in the contract/agreement
- have read and understood the legislation, orders, policies and procedures relating to information security within the QPS
- will abide by those provisions and understand that if they breach the agreement/contract they will be disciplined or dismissed.

Provisions must also be made to prevent members from signing the acknowledgment without reading it. The most suitable mechanism is to have a supervisor/manager witness the signing and also sign the acknowledgment, stating that the member has demonstrated that he/she has read the acknowledgment and fully understood it. Where a supervisor/manager is not satisfied that the member has the necessary understanding and knowledge of the legislation, orders, policies and procedures relating to computer information security, access should not be granted until the member completes appropriate training and education on information security.

It is important that the acknowledgment be renewed from time to time to ensure that members do not forget their obligations regarding information security. The nature of policing is such that many employees, particularly police officers, may stay with the Service for their entire career. Employees need to be reminded of their obligations throughout their career and advised of changes to information-security policies and practices. As more and more information becomes available to members on the computer systems, the QPS will need to be vigilant in renewing its members' agreement to adhere to the information-security policies.

It is impractical to suggest that the QPS should have all employees renew their acknowledgment each year. It will be administratively easier to have this renewal process integrated into an already existing process. One such process is the application to entitle the individual to be an authorised user of the QPS computer systems.

Members are required to apply for access, or renewal of access, to computer corporate/mainframe systems to the ISS. As part of the application process, it would be effective to have members, and their respective supervisors/managers, sign and renew their acknowledgment. Such a requirement would be timely, given that the member is about to be granted access to a computer system/database that contains confidential information. It also satisfies the ISS requirement that the applicant be suitably aware of, and trained in, information security as it relates to computer use.

RECOMMENDATION 6.12 — RAISING AWARENESS OF INFORMATION SECURITY AND INDIVIDUAL ACCOUNTABILITY

6.12.1 That, in response to this report, the Commissioner of Police issue a notice to all members, addressing the issues arising from this Inquiry, areas of concern and policy developments in respect of information security.

6.12.2 That the Queensland Police Service require all members to sign an acknowledgment stating that they:

- agree to the information-security policies as specified
- fully understand that the QPS computer system is not for personal use and, therefore should only ever be accessed and used in the performance of official police work

CCC EXHIBIT

- have read the legislation and will abide by the legislation, orders, policy and procedural rules and guidelines on computer use and access, and release of information
- understand that a breach of the terms of the contract/agreement will result in criminal and/or disciplinary action and possible dismissal.

To ensure that no significant administrative burden is placed on the QPS, implementation should be progressive and be applicable to all new recruits from January 2001.

6.12.3 That a supervisor or manager witness the signing of the acknowledgment, and also attest that the member has demonstrated that he/she has read the contract/agreement and fully understands its content.

6.12.4 That, where a supervisor or manager is not satisfied that a member has the necessary understanding of legislation, orders, policies and procedures relating to security of computer information, access should not be granted until the member completes appropriate training and education.

6.12.5 That all members be required to re-sign their acknowledgment when they request new, changed or renewed access to a mainframe/corporate system or database.

TRAINING AND EDUCATION IN INFORMATION SECURITY

The training provided to recruits in the PROVE and POCC programs is comprehensive with regard to computer use and information security (described on pages 49–50). However, the training programs for more senior members of the QPS concentrate more on ethics training than information security and effective supervisory practices.

In addition, the preliminary findings of a recent survey on policing and IT (Chan, J. et al. forthcoming) within the QPS show that as officers progress in rank they spend less time using computers/databases, are more likely to see themselves as incompetent at using IT and are less likely to receive computer training. The preliminary findings demonstrate the need to ensure that senior officers are receiving the necessary training. If supervisors are to supervise their subordinates effectively in computer use, they must be proficient at using and understanding the systems themselves and, arguably, must be better trained in information security. Supervisors must also understand, and be able to apply, the principles of risk management. The QPS has adopted risk-based assessment as a critical management function. It is important that supervisors can apply risk-management principles in the context of information security.

In its written submission, the QPS stated that:

> The strongest protection [for information security] comes from education and training programs that emphasise the responsibility members have for maintaining secure systems and processes. The Service will examine its training programs in light of any outcomes of the present inquiry, to identify means of re-emphasising the responsibilities of staff in relation to the information they have access to. (QPS submission 2000, p. 26)

It should be noted that the QPS did not claim that training and education were the only components of a program aimed at preserving information security, but that it was the strongest component.

The CJC does not agree that the strongest protection comes from education and training programs. It is difficult to ascertain which components of a strategic approach provide the greatest prevention and deterrent effect. The CJC is of the view that it is the combined effect of the full collection of complementary initiatives, policies, procedures and practices that affords the strongest protection and provides the necessary prevention and deterrent effects. The QPS must be careful not to place too much reliance on training and education to ensure compliance with information-security orders, policies and procedures. As was observed during the Inquiry, one officer who had received extensive training in computer use and information security conducted over 300 inappropriate checks on the computer system. This officer quite clearly knew of his obligations and in fact had written an assignment citing many examples of inappropriate use.

Nevertheless, training and education are important components of an overall information-security strategy. As computers are increasingly relied upon in police work, the training in computer use and information security must form part of the training and education programs for members later in their career. The QPS computer system is continually evolving, and therefore requires continuity in training for all ranks and positions in the Service. As the systems develop, so should the information security policies. Managers, in particular, should be familiar with the changes and able to implement supervisory and risk-management processes to ensure compliance.

CCC EXHIBIT

The QPS indicated in its submission that it was developing a CAP (Competency Acquisition Program) module that was specifically concerned with computer use and information security. The CJC urges the QPS to complete the module, as it is important to provide further training in the area for civilian members of the QPS and remedial training for those members who are assessed as in need of it.

RECOMMENDATION 6.13 — EXTENDING INFORMATION SECURITY

6.13.1 That the Queensland Police Service incorporate, in higher education and training programs, particularly those catering for supervisors and managers, training sessions/modules on computer use, information security and supervision of computer use by subordinates.

6.13.2 That the Queensland Police Service educate managers and supervisors on the application of the principles of risk management to develop processes for the effective monitoring and supervision of subordinate staff in the use of, and access to, the police computer system.

6.13.3 That the Queensland Police Service complete the development of the Competency Acquisition Program module on computer use and information security.

CONCLUSION

Management of information security is becoming an increasingly high priority for organisations. This is not surprising, given that information is well recognised as a valuable asset to the organisation. The advent of information technology has resulted in significant increases in the efficiency of information systems, facilitated the development of open communication systems and provided many individuals with immediate access to information that allows them to perform their duties more effectively.

With these rapid advances has come greater risk. This risk has been made even greater because of the lag in technology designed to mitigate those risks and the delay in organisations' recognising the need to have management of strong information security. In assessing the QPS system for managing information security, all of the following were considered:

- the Australian and New Zealand Standard on Information Security Management (AS/NZS 4444.1:1999) in combination with the review of current literature in best practice
- the issues raised through public submissions and presentation of evidence
- the lessons to be learnt from other jurisdictions, particularly the NSW Police Service
- the final comments and submission made by the QPS.

In this chapter, recommendations have been made that represent both an organisational and a technological response to the issues raised. A significant number of recommendations have been made to 'close any gaps' in policy and procedure (e.g. policy to prohibit leaving open computer terminals unattended, proper disposal of paper copies of in-confidence material and mandatory recording of reasons for transactions).

It has also been recommended that the location of the ISS be reviewed, giving consideration to its placement within the ESC. Technological recommendations for the development of features such as 'alert' monitoring to improve detection systems have also been made. Finally, it has been recommended that the QPS commence a program of systematic and ongoing internal audit on access and use of QPS computer systems. Such a program should have both random and targeted components. This will allow the Service to be proactive in its monitoring of this type of misconduct.

CCC EXHIBIT