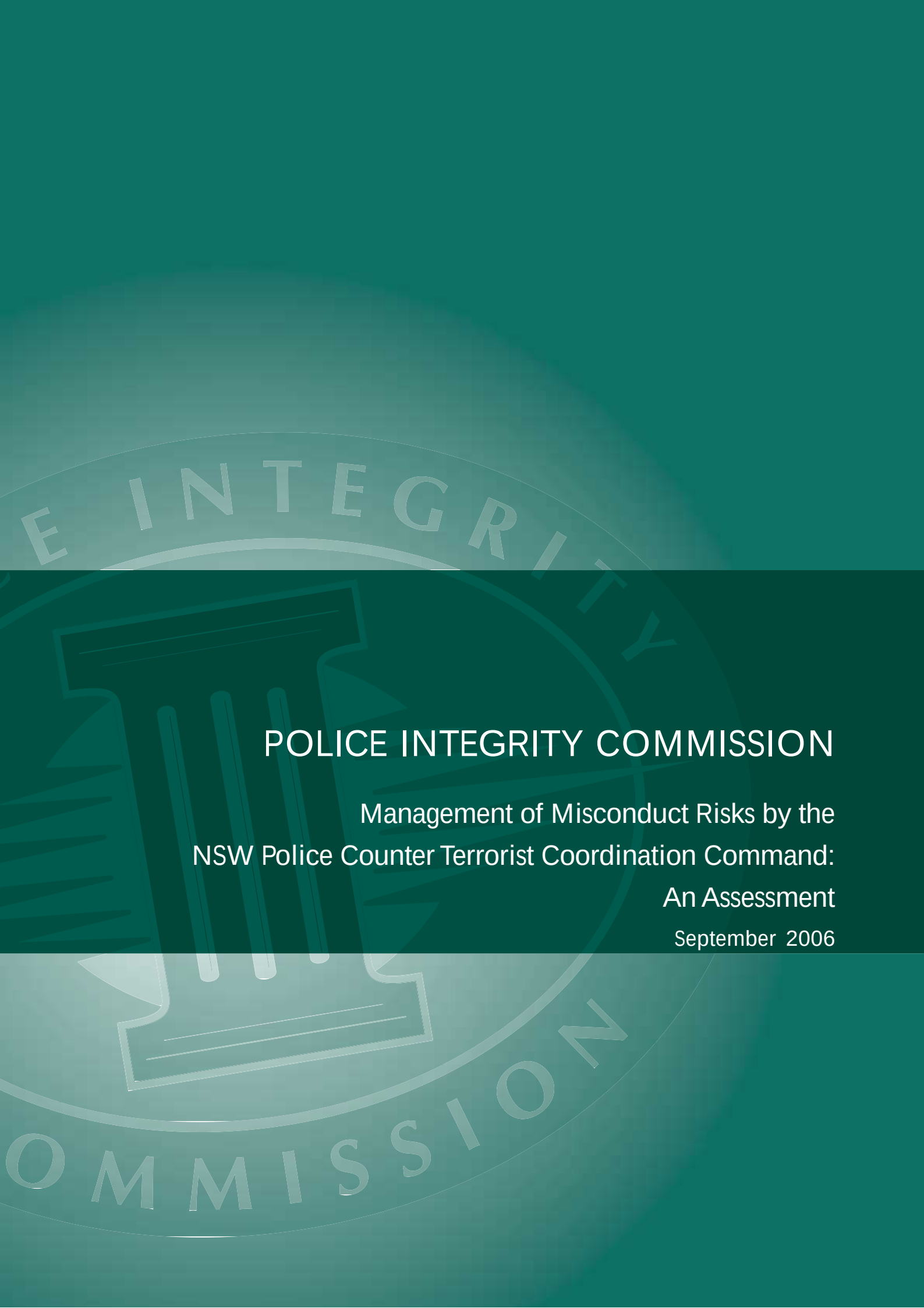


POLICE INTEGRITY COMMISSION

Management of Misconduct Risks by the NSW Police Counter Terrorist Coordination Command: An Assessment

September 2006

Management of Misconduct Risks by the NSW Police Counter Terrorist Coordination Command: An Assessment

SEPTEMBER 2006

ISBN 1 74003 143 1

© Police Integrity Commission 2006

Address: Level 3, 111 Elizabeth St, Sydney 2000
Postal: GPO Box 3880, Sydney NSW 2001
Telephone: [61 2] 9321 6700 or 1800 657 079 (toll free)
Facsimile: [61 2] 9321 6799
Email: contactus@pic.nsw.gov.au
Website: www.pic.nsw.gov.au



POLICE INTEGRITY COMMISSION

MANAGEMENT OF MISCONDUCT RISKS BY THE NSW POLICE COUNTER TERRORIST COORDINATION COMMAND:

AN ASSESSMENT

September 2006

CONTENTS

Abbreviations iv

SUMMARY v

1. INTRODUCTION 1
   - 1.1 Overview 1
     - The role of the Police integrity Commission 1
     - The transition: Special Branch – Protective Security Group – Counter Terrorist Coordination Command 1
     - Inquiry by Parliamentary Committee 2
   - 1.2 Why did the Commission undertake this assessment? 3
   - 1.3 Purpose of this assessment 3
   - 1.4 Structure of this report 3

2. BACKGROUND 5
   - 2.1 Special Branch 5
     - History and role 5
     - Identified misconduct 6
     - Identified need for safeguards and oversight for future units 7
   - 2.2 Protective Security Group 9
     - History and role 9
     - Identified need for oversight 10
     - Nature of legislated oversight regime 12
   - 2.3 Counter-Terrorist Coordination Command – A new command incorporating the functions of the Protective Security Group 13
     - History and role 13
     - Operational context 14
   - 2.4 Parliamentary Committee – Two related inquiries 15
     - February 2004 inquiry 15
     - March 2006 inquiry 17
     - The Commission's submission 17
   - 2.5 Summary of key points 18

3. LEGISLATIVE CHANGES IN THE AREA OF COUNTER-TERRORISM POLICING 19
   - 3.1 Referral of terrorism powers to the Commonwealth 19
   - 3.2 Identified need to balance powers with accountability 20
   - 3.3 Powers provided by NSW legislation 21
   - 3.4 Authorisation and accountability requirements incorporated in NSW legislation 22
     - Authorisation 22
     - Accountability requirements 22
   - 3.5 Summary of key points 28

4. MISCONDUCT RISK ASSESSMENT 29
   - 4.1 Misconduct risks 29
   - 4.2 How the Commission undertook this assessment 29
     - Objectives of the assessment 30

Information collected 30
Limitations of the assessment 32
4.3 Summary of key points 32

5. RISK MANAGEMENT 39
5.1 Providing some context 39
Risk Management Guidelines 39
Misconduct Risk Management Guidelines 41
Research on risk management in law enforcement 43
5.2 Processes used by NSW Police and the CTCC 44
NSW Police – Corporate strategies 45
CTCC – Command-level strategies 49
5.3 Observations 54
The corporate approach 54
The command-level approach 55
5.4 Summary of key points 56

6. COUNTER TERRORIST COORDINATION COMMAND: FUNCTIONS AND ASSOCIATED RISKS 57
6.1 Role, functions and structure 57
Background 57
Mission and role 57
Charter 58
Structure of the CTCC 59
Features of the CTCC's work 60
6.2 Misconduct risks potentially faced by officers working in the CTCC 62
Potential misconduct risks identified by NSW Police 62
Potential misconduct risks identified through other sources 64
6.3 Summary of key points 72

7. TREATING THE MISCONDUCT RISKS 73
7.1 Background 73
7.2 Treating misconduct risks identified by the CTCC 73
Sources of information 73
Strategies in place 74
Proposed strategies 82
Monitoring the effectiveness 82
7.3 Strategies to minimise the likelihood of repeating the failings of the former Special Branch 83
Adherence to charter and accountability 83
Target selection and information collection 84
Informant management 84
Recruitment 85
7.4 Preparing CTCC officers for the misconduct risks they might face 85
Information provided by NSW Police at the corporate level 86
Information provided by the CTCC at the command level 86
The CTCC induction program 86
7.5 Protective Security Group Corruption Prevention Plan 88
7.6 Observations 89
7.7 Summary of key points 91

8. OVERSIGHT PROVIDED 93
8.1 Background – Oversight of the operation of the former PSG 93
8.2 Current oversight of the CTCC 93
8.3 Perceptions of benefits and disadvantages of the oversight regime used for the PSG 94
Annual audit by NSW Police Audit Group 94
Oversight by an external agency such as the Commission 95
8.4 Suggestions for nature of oversight required by the CTCC 96
8.5 Oversight of other NSW Police commands 97
Self-assessment using the CMF 97
Organisational Review and Support 97
8.6 Observations 98
8.7 Summary of key points 99

9. ASSESSMENT 101
9.1 Relevant considerations 101
Do the misconduct risks faced by the CTCC differ from those faced by other commands? 102
What mechanisms are in place to minimise any CTCC misconduct risks that are different from those faced by other commands? 105
What lessons have been learnt from the investigations into the former Special Branch? 107
What features of oversight are desirable and what oversight is currently provided? 108
9.2 Opportunities for strengthening resistance to misconduct 109
Strengths 109
Opportunities 110
9.3 Oversight required 112
A more targeted form of monitoring than that previously required for the PSG 112
Focus on appropriate targeting and appropriate retention (and disposal) of information 112
The way forward 113

GLOSSARY 115

REFERENCES 119

APPENDICES 123
Appendix 1: Role and functions of the Police Integrity Commission 123
Appendix 2: Chronology 129
Appendix 3: Summary of special legislative provisions in relation to terrorism 133

ABBREVIATIONS

AFP	Australian Federal Police
AMCRAN	Australian Muslim Civil Rights Advocacy Network
ASAP	Agents Scheduling and Personnel (database)
ASIO	Australian Security Intelligence Organisation
ASNET	Australian Secure Network (Commonwealth classified security email system)
C@ts.i	Customer Assistance Tracking System (NSW Police complaints management system)
CMF	Command Management Framework (NSW Police self-assessment audit tool)
CMT	Complaints Management Team (NSW Police)
Commission	Police Integrity Commission (NSW)
Committee	Parliament of NSW Committee on the Office of the Ombudsman and the Police Integrity Commission
COPS	Computerised Operational Policing System (NSW Police data system)
CTCC	Counter Terrorist Coordination Command (unit of NSW Police that reports to the Assistant Commissioner Counter Terrorism and Public Order Management)
CTMC	Counter Terrorist Management Committee
HMIC	Her Majesty's Inspectorate of the Constabulary (UK)
ICAC	Independent Commission Against Corruption (NSW)
JCTT	Joint Counter-Terrorism Teams
MOU	Memorandum of Understanding
NCIS	National Crime and Intelligence Service (UK)
NCTC	National Counter Terrorism Committee
NSW	New South Wales
NSW CC	New South Wales Crime Commission
OCA	Officer Complaint Analysis (NSW Police)
ORC	Operations Review Committee (committee within the Counter Terrorism Coordination Command)
PIC Act	*Police Integrity Commission Act 1996*
PMV	Politically motivated violence
PORS	Public Order and Riot Squad (unit of NSW Police that reports to the Assistant Commissioner Counter Terrorism and Public Order Management)
PSC	Professional Standards Command (unit of NSW Police)
PSG	Protective Security Group (former unit of NSW Police)
PSRG	Protective Security Response Group (proposed name for unit of NSW Police which was subsequently called Protective Security Group)
Royal Commission	Royal Commission into the NSW Police Service
SOPs	Standard Operating Procedures
SPG	State Protection Group (unit of NSW Police that reports to the Assistant Commissioner Counter Terrorism and Public Order Management)

SUMMARY

This assessment focuses on the nature of the work undertaken by the NSW Police Counter Terrorist Coordination Command (the CTCC) and on the management of any misconduct risks associated with this work. It does not examine the conduct of individual officers. The Police Integrity Commission (the Commission) undertook this assessment to consider what, if any, special oversight or monitoring arrangements are needed to adequately manage the misconduct risks that result from the nature of the work undertaken by officers in the CTCC.

WHY THE CTCC IS OF PARTICULAR INTEREST

The Commission's interest in the misconduct risks of the CTCC has stemmed from a recognised need for the oversight of the NSW Police units which have provided intelligence about politically motivated violence (including terrorism) in the past. The Commission has no reason to believe that individual officers who are appointed to work in the CTCC are more likely to engage in misconduct than officers who work in other NSW Police commands.

The CTCC is not the first unit of NSW Police that has had a responsibility for counter-terrorism policing. For half a century, the Special Branch was responsible for providing intelligence concerning politically motivated violence, including terrorist activity. The Special Branch was disbanded in March 1997 after evidence was heard in the Royal Commission into the NSW Police Service (the Royal Commission) concerning abuses of power and a lack of accountability including, amongst a number of other concerns, officers gathering information and maintaining files on people who posed no threat of politically motivated violence, and a lack of satisfactory procedures for the management and payment of informants. (For further information on the history, role and documented weaknesses of the former Special Branch refer to Section 2.1 in Chapter 2.)

The then Commissioner of Police, the Royal Commission and the NSW Government each identified the need for special oversight for any unit that was to replace the Special Branch. When establishing the Protective Security Group (the PSG) to replace the disbanded Special Branch, the then Minister for Police noted that the NSW Government held the view that any unit undertaking the functions that were to be undertaken by the PSG should be subject to high standards, and an even higher level of scrutiny than other commands. To provide this oversight the NSW Government introduced legislation that required NSW Police to conduct annual audits of the operations of PSG and required the Commission to monitor and report on those audits. (For further information on the history and role of the PSG, the identified need for oversight of any unit carrying out such functions and the nature of the legislated oversight see Section 2.2 of Chapter 2.)

In March 2003, the PSG's functions were absorbed into the newly created CTCC (see Section 2.3 in Chapter 2) and the annual audits ceased. This resulted in a legislative anomaly, whereby the sections of the *Police Act 1990* concerning the conduct of annual audits of the PSG and sections of the *Police Integrity Commission Act 1996* concerning the monitoring of those audits no longer had practical application. There had been no explicit policy decision by Government determining that the Commission's

oversighting function or the need for regular audits of the work previously undertaken by the PSG, or the work currently undertaken by the CTCC, should come to an end.

The Parliament of NSW Committee on the Office of the Ombudsman and the Police Integrity Commission (the Committee) subsequently established two related inquiries. Amongst other issues, these inquiries sought to examine the need for special oversight or monitoring arrangements for the CTCC and the form any required oversight should take. In its submission to the first of these inquiries, the Commission indicated that any position regarding future arrangements for the oversight of the CTCC should be based on a clear understanding of the risks for police misconduct associated with the CTCC's activities and structure. The Committee agreed and the Commission undertook this assessment. (For more information about the Parliamentary Committee's inquiries and the Commission's submission see Section 2.4 in Chapter 2.)

ASSESSMENT METHODOLOGY

The Commission collected information about four main areas:

- the strategies used corporately by NSW Police and at the command-level by the CTCC to identify, to assess and to decide how to treat risks in general, and misconduct risks in particular (summarised in Chapter 5)
- the nature of the work undertaken by the CTCC and the misconduct risks associated with this work (summarised in Chapter 6)
- the strategies used to treat (manage or mitigate) these misconduct risks (summarised in Chapter 7), and
- oversight arrangements currently in place and opinions about the most appropriate oversight arrangements for the future (summarised in Chapter 8).

The Commission used a diverse and complementary range of sources to gather relevant information. This included obtaining information from NSW Police by formally and separately seeking written NSW Police corporate-level views and CTCC command-level views on topics of interest and conducting structured interviews with key staff of the CTCC. The Commission also examined and reviewed a range of documents including published literature, NSW legislation pertaining to counter-terrorism policing, complaints made about officers assigned to the CTCC, available judgments relating to prosecutions of terrorism suspects, and relevant NSW Police policies and other documentation. (See Chapter 4 for additional information about the process the Commission followed to conduct its assessment.)

LEGISLATIVE CHANGES IN COUNTER-TERRORISM POLICING

The NSW counter-terrorism legislation which specifically affects police powers is the *Terrorism (Police Powers) Act 2002* and its subsequent amendments:

- *Crimes Legislation Amendment (Terrorism) Act 2004*
- *Terrorism Legislation Amendment (Warrants) Act 2005*
- *Terrorism Legislation Amendment (Preventative Detention) Act 2005*.

When introducing this legislation, the NSW Government has emphasised the need to balance police powers with accountability measures and safeguards.

The police powers, the authorisation process and the accountability requirements that are provided by the *Terrorism (Police Powers) Act 2002* and its subsequent amendments are summarised in Table 3.1 in Chapter 3. These powers are not restricted to officers employed in the CTCC. With the exception of the powers concerning covert search warrants, the other powers provided in this legislation can be employed by any NSW Police officer, though the use of these powers can be authorised by only a relatively small number of individuals and can only be authorised under quite specific circumstances. To the extent that these powers provide additional misconduct risks, such misconduct risks would not be confined to officers working within the CTCC. (For further information see Chapter 3 and Appendix 3.)

CURRENT CTCC MISCONDUCT RISK MANAGEMENT

CTCC functions

Notwithstanding the name of the command, the work undertaken by the CTCC is broader than counter-terrorism policing. The CTCC is composed of three different work units: the Dignitary Protection Unit, the Intelligence Unit, and the Investigations Unit. While the CTCC's work is also broader than that of the former PSG and that of the former Special Branch, it incorporates all of the functions of the former PSG and the former Special Branch. This includes the functions that were associated with the documented problems of the former Special Branch and the functions of the PSG that were seen to require special monitoring.

The CTCC's work has a preventative focus. The nature of the information collected to prevent politically motivated violence (including terrorism) and to assist in dignitary protection, while a fundamental aspect of the CTCC's functions, has in the past been associated with misconduct. (For further information of the CTCC's role, functions and structure see Section 6.1 in Chapter 6.)

Misconduct risk management processes

The Command Management Framework (CMF), which provides templates for a 'risk-based self-assessment audit' is the core tool that NSW Police advises it uses for identifying, documenting and managing risks, including misconduct risks. Individual commands are responsible for tailoring the CMF to their own requirements and are responsible for administering the CMF. Like other commands, the CTCC uses the CMF as the basis of its risk management.

However, the CMF is only one part of the CTCC's misconduct risk management process. In its responses to the Commission's questions, the CTCC has advised that it has a number of committees that are responsible for identifying, reducing and/or managing misconduct risks. It has listed fourteen different processes that it uses to identify misconduct risks as well as a number of factors which could trigger the command to review the misconduct risks faced by its officers. Overall, the picture the CTCC provides of its risk management strategies is one incorporating a number of discrete elements where any interrelationships between the elements are not explicitly stated. The absence of documentation of the CTCC's risk management strategies

means that it is difficult to assess how cohesive or comprehensive its current misconduct risk management processes are. (For further information see Chapter 5.)

CTCC misconduct risks

The Commission is of the view that like officers from any command, officers who work in the CTCC face a range of misconduct risks. While most of these misconduct risks (such as the unauthorised release or misuse of confidential information or improper associations) are pertinent to officers working in other commands, some misconduct risks arising in the CTCC environment (such as the potential for inappropriate targeting or for maintaining files on those who are unlikely to pose a threat of politically motivated violence) would be uncommon in other commands.

At the time the Commission collected information for this assessment, there was no consolidated list of the misconduct risks that might face officers working in the CTCC. Table 6.1 in Chapter 6 provides a listing of the different misconduct risks identified through different sources. (For further information on misconduct risks potentially faced by officers working in the CTCC, see Section 6.2 in Chapter 6.)

Treatment of misconduct risks

Unlike the former Special Branch, the CTCC does not rely on command-specific systems, Instead it uses NSW Police corporate systems for information management, informant (or source) management, and for recruitment. Some of these corporate systems include facilities which enable regular audits to be conducted.

In addition to the use of corporate systems, the misconduct risk treatment strategies described by the CTCC include: physical security, use of a panel rather than individuals to decide which information should be collected, supervision and record keeping in relation to investigations, rotation of officers, and audits to both deter and detect individual examples of misconduct. The CTCC has also advised that because its officers work closely with officers from other agencies such as the AFP and ASIO, the work of CTCC officers is subject to being observed by officers from these other agencies.

The minutes of the CTCC's Complaints Management Team (CMT) meetings contain examples of where the CTCC's CMT has looked at the wider implications of individual complaints and taken steps to tackle the underlying issues.

However, the information provided by the CTCC did not link its treatment strategies, or its CMF, to the specific misconduct risks that it has identified in its written response. Hence it is not clear whether or not the CTCC has strategies in place for each of the misconduct risks it has identified. From the information provided, it is not possible to assess the effectiveness of the CTCC's misconduct risk treatment strategies.

CTCC officers are not told of the specific misconduct risks they might face in their work. Nor are they told of the documented problems associated with the way the former Special Branch discharged functions not dissimilar to those performed by the CTCC. (For further information on the treatment of the CTCC's misconduct risks refer to Chapter 7.)

Oversight

Unlike the former PSG, the CTCC is not the subject of any special legislated oversight requirements. Much of the oversight of the work of the CTCC, like the oversight of the work of other NSW Police commands, is currently based on supervision and self-assessment audits from within the command. (For further information see Chapter 8.)

THE WAY FORWARD

While the CTCC has introduced processes to manage some of its misconduct risks, the Commission considers that there are opportunities to further strengthen the CTCC's capacity to resist misconduct (see Section 9.2 in Chapter 9). The Commission considers that the way forward should include the following three elements:

1. the CTCC (at the command level) and NSW Police (at the corporate level) documenting their recognition of the inherent misconduct risks for any unit that undertakes the work of the former Special Branch and documenting the lessons for those currently undertaking this work, to be learnt from the investigations undertaken into the work of the former Special Branch
2. the CTCC more generally strengthening its capacity to identify and respond to current as well as future misconduct risks by:
    - preparing and implementing a documented misconduct risk management plan
    - equipping its officers for the misconduct risks they may face through their work in the CTCC by informing them of the specific misconduct risks they might encounter in their work and how these officers should respond if they find themselves in such circumstances, and
3. NSW Police to impose some specific monitoring of the practices and procedures used by the CTCC to manage targeting and information retention (and disposal).

The Commission does not wish to prescribe the form of monitoring to be used by NSW Police. This is, and should be, a management issue for NSW Police. However, the Commission would be concerned if there were not clearly defined, transparent procedures developed and promulgated. At this stage, the Commission does not see that oversight by an external agency needs to be mandated. The current absence of a legislative provision for auditing and monitoring does not in any way preclude the Commission from exercising its functions and powers in connection with the CTCC. Also the management of any complaints about CTCC officers remains subject to the oversight of the NSW Ombudsman's Office.

The Commission will retain an interest in this area until it is satisfied with the systems put in place by the CTCC and by NSW Police to manage these potential misconduct risks.

1. INTRODUCTION

1.1 OVERVIEW

This report describes an assessment of the management of the misconduct risks faced by officers working in the NSW Police Counter Terrorist Coordination Command (the CTCC). This assessment was undertaken by the Police Integrity Commission (the Commission) to inform decisions concerning what, if any, special oversight of the CTCC is required to adequately manage the misconduct risks that result from the nature of the work undertaken by officers in this command.

THE ROLE OF THE POLICE INTEGRITY COMMISSION

The principal functions of the Commission can be summarised as 'detecting, investigating and preventing serious police misconduct in NSW'. In addition, the Commission is responsible for auditing and monitoring particular aspects of NSW Police operations and procedures. (Further information about the Commission's role, functions and approach is provided in Appendix 1.)

Of particular relevance to this assessment, section 14(e) of the *Police Integrity Commission Act 1996* (the PIC Act) requires that the Commission monitors and reports on the conduct and effectiveness of the annual audits of the NSW Police Protective Security Group (the PSG). These annual audits are required to be conducted by NSW Police under Part 3 of the *Police Act 1990*.

THE TRANSITION: SPECIAL BRANCH - PROTECTIVE SECURITY GROUP – COUNTER TERRORIST COORDINATION COMMAND

While the attacks on the World Trade Centre in New York and on the Pentagon in Washington focussed the world's attention on terrorism more keenly than ever before, policing activities to counter politically motivated violence (including terrorism) as well as the discussion of the oversight of such policing activities predate the horrors of 11 September 2001.

In NSW, for half a century, the Special Branch was responsible for providing intelligence concerning politically motivated violence, civil disorder, terrorist and extremist activity. The Special Branch was disbanded in March 1997 after evidence was heard in the Royal Commission into the NSW Police Service (the Royal Commission) concerning abuses of power and a lack of accountability.

The PSG was established to replace the disbanded Special Branch. The Commissioner of Police, the Royal Commission and the NSW Government each identified the need for special oversight for the PSG. When establishing the PSG, the then Minister for Police noted that the 'Government remains of the view that any unit with these unusual functions should be subject to high standards, and an even higher level of scrutiny than most' (NSW Legislative Assembly, 23 June 1998, p. 6254). To provide this oversight the NSW Government introduced legislation that required NSW Police to conduct annual audits of the operations of the PSG and required the Commission to monitor and report on those audits.

In March 2003, the PSG's functions were absorbed into the newly created CTCC. Although it was not known to the Commission at the time, the effect of this change was to render the Commission's function to monitor and report on the audits of the PSG (section 14(e) of the PIC Act) redundant. It is important to note that there was no explicit policy decision by Government determining that the Commission's oversighting function or the need for regular audits of the work previously undertaken by the PSG, or the work currently undertaken by the CTCC, should come to an end.

This resulted in a legislative anomaly, whereby the sections of the *Police Act 1990* concerning the conduct of annual audits of the PSG and sections of the PIC Act concerning the monitoring of those audits no longer have practical application. These provisions have not, at present, been amended or replaced by similar provisions to ensure monitoring and scrutiny of the CTCC's activities.

INQUIRY BY PARLIAMENTARY COMMITTEE

Concerned by the ambiguity of the legislative situation, in February 2004 the Parliament of NSW Committee on the Office of the Ombudsman and the Police Integrity Commission (the Committee) commenced an inquiry into the Commission's jurisdiction to oversight the PSG. In its media release to announce this inquiry, the Committee stated that it had 'determined to conduct a parliamentary inquiry touching on the oversight of the NSW Police Counter Terrorism Coordination Command (CTCC)'. This media release provided the following summary of the background to this inquiry:

> The Protective Security Group (PSG) replaced Special Branch in 1998, said Committee Chairman, Paul Lynch MP (Member for Liverpool).
>
> The PSG, however, was subject to strict accountability set out in legislation. This included annual audits, which NSW Police had to report to the Police Integrity Commission (PIC).
>
> The PIC had statutory responsibility to monitor and report on the conduct and effectiveness of the annual PSG audits.
>
> The PSG was incorporated into the CTCC in late 2002.
>
> There now seems to be a significant gap in the oversight of the bodies carrying out the PSG work (Parliament of NSW Committee on the Office of the Ombudsman and the Police Integrity Commission 2004).

In its written submission to this inquiry, the Commission identified the need to develop a better understanding of the nature of the misconduct risks faced by those working in the CTCC. The Committee endorsed the Commission's proposal to conduct a misconduct risk management assessment of the CTCC and determined to await the outcomes of that assessment before concluding its inquiry.

1.2 WHY DID THE COMMISSION UNDERTAKE THIS ASSESSMENT?

The Commission's interest in the management of misconduct risks faced by officers working in the CTCC is a result of the following combination of factors:

- the Commission's broad role in preventing serious police misconduct
- the Commission's specific role in monitoring and reporting on the NSW Police annual audits of the former PSG
- the NSW Government's observation that functions undertaken by the PSG - which was succeeded by the CTCC - required high levels of scrutiny, and
- the Commission's undertaking to conduct a risk management assessment to inform the Committee's inquiry into the Commission's jurisdiction to oversight the PSG and the Committee's decision to await the outcomes of this assessment prior to concluding its inquiry.

1.3 PURPOSE OF THIS ASSESSMENT

The Commission seeks to provide advice to the Committee's inquiry as to what, if any, special oversight or monitoring arrangements are needed to adequately manage the misconduct risks in the CTCC. To inform its advice, the Commission is conducting this assessment to develop a better understanding of:

1. What are the misconduct risks associated with the functions of the CTCC?

2. How well is NSW Police identifying, assessing and managing misconduct risks faced by those working in the CTCC?

1.4 STRUCTURE OF THIS REPORT

The first four chapters of this report contain introductory information that provides a context for this assessment of the management of misconduct risks by the CTCC:

- Chapter 2 provides a more detailed description of the background to the Commission's decision to undertake this assessment. It describes the history and role of each of the Special Branch, the PSG and the CTCC to enable consideration of the similarities and differences in the functions undertaken by these different NSW Police units. It outlines the types of problems associated with the operations of the former Special Branch that were identified by the Royal Commission and subsequently by the Police Integrity Commission. It describes the nature of the safeguards and oversight proposed by the Commissioner of Police and the Royal Commission and the oversight legislated by the NSW Government for the agency that was to replace the Special Branch. It also provides further information about the inquiries being conducted by the Committee.

- Chapter 3 outlines the nature of policing powers and associated accountability measures introduced by NSW legislation in the area of counter-terrorism policing.
- Chapter 4 clarifies what the Commission means by 'misconduct risk' and describes the methodology that the Commission used to undertake its assessment of the management of misconduct risks by the CTCC.

The following four chapters describe the information collected in terms of the role and functions of the CTCC; risk identification, assessment and management procedures within NSW Police in general, as well as risk identification, assessment and management procedures within the CTCC:

- Chapter 5 describes the processes that NSW Police (corporately) and the CTCC (at the command level) advise are used to identify, assess and manage risk in general and misconduct risk in particular. To provide a context in which to consider these processes, Chapter 5 also includes a brief review of the guidance available concerning risk management and a review of research on the use of risk management and misconduct risk management within other law enforcement agencies
- Chapter 6 describes the role, functions and structure of the CTCC and the associated misconduct risks
- Chapter 7 describes the strategies that the CTCC uses to treat its misconduct risks
- Chapter 8 describes current oversight provisions and key CTCC officers' views of the monitoring or oversight required to adequately manage potential misconduct risks facing the CTCC.

The final chapter (Chapter 9) provides the Commission's views. This chapter commences with a discussion of whether the misconduct risks faced by the CTCC differ from those faced by other commands, the mechanisms that are currently in place to address any CTCC misconduct risks that are different from those faced by other commands, the lessons that have been learnt from the investigations into the former Special Branch, the desirable features of oversight and the oversight currently provided. Several opportunities for the CTCC to further strengthen its capacity to resist misconduct are identified. The chapter concludes with a statement of the Commission's position concerning appropriate oversight.

2. BACKGROUND

This chapter provides a more detailed description of the background to the Commission's decision to undertake this assessment by outlining:

- the nature of problems documented in the management of the former Special Branch (Section 2.1)
- the 'unusual functions' and legislated oversight regime regarded as necessary for the PSG (Section 2.2)
- the Counter Terrorism Coordination Command – a new command incorporating the functions of the PSG (Section 2.3), and
- the inquiries commenced by the Committee (Section 2.4).

A timeline of the inquiries into the work of Special Branch, the establishment and disestablishment of relevant units of NSW Police, the introduction of relevant legislation and major international terrorism attacks is provided in a Chronology in Appendix 2.

2.1 SPECIAL BRANCH

HISTORY AND ROLE

Special Branch operated from 1948 until March 1997, when it was disbanded by the Commissioner of Police following evidence put before the Royal Commission. Over time, its work changed from concentrating on the 'subversive' conduct of communist and related groups to a focus on the protection of dignitaries. As documented in an earlier Commission report:

> The Special Branch had operated from 1948, concentrating its efforts on the 'subversive' conduct of communist and related groupings. As the hysteria of the Cold War abated, less attention was paid to such matters. Because its records addressed an overlap between functions of intelligence and the protection of VIPs, the Special Branch also became the manager of close personal protection arrangements for those VIPs.
>
> The principal focus of the Special Branch had shifted to the protection of VIPs, with this constituting about seventy-five percent of the work performed by the time of the Branch's closure. The intelligence gathering activities had drifted towards politically motivated violence, thought to be a tactic of radical groupings (Police Integrity Commission 1998, p. ii).

The Mission Statement of the Special Branch at the time the Branch was disbanded was as follows:

> a. to provide relevant, current and specialised strategic and tactical intelligence concerning politically motivated violence and/or civil disorder, terrorist and extremist activity, and

b. to plan and implement security procedures to ensure the safety of VIPs and property (Police Integrity Commission 1998, p. 10).

As at 1978, Special Branch was divided into three, sometimes overlapping, divisions:

i. that dealing with communists and 'revolutionary' socialist organisations and other organisations through which they exert influence as well as 'right wing' racist groups

ii. that dealing with 'the radical left' including revolutionary and terrorist organisations

iii. that dealing with ethnic communities and extreme right wing groups and certain university based organisations and trade unions (Privacy Committee 1978, p. 3).

The activities of the Special Branch at the time it was disbanded have been described as falling into a number of broad categories:

- provision of VIP security
- attending demonstrations
- conducting or assisting major investigations
- ministerial enquiries and employment checks, and
- information gathering (Parliament of NSW Committee on the Office of the Ombudsman and the Police Integrity Commission 2005, p. 14).

IDENTIFIED MISCONDUCT

Aspects of the conduct of the Special Branch were examined initially by the Royal Commission and subsequently by the Police Integrity Commission. Record keeping practices of the Special Branch had also been examined by the Privacy Committee in 1978 as part of its review of criminal records in NSW (Privacy Committee 1978).

In the course of its inquiries into the paedophile segment of its reference, the Royal Commission received evidence concerning the Special Branch. The Royal Commission identified the following aspects of the operation of Special Branch as 'matters for serious concern':

- the disregard of its charter;
- the fact that it seemed accountable only to itself, operating under a cloak of secrecy;
- the possible abuse of allowances and of monies ostensibly payable to informants or sources of intelligence;
- lax and inconsistent record keeping practices and woefully inappropriate systems for recording payments and allowances;
- long lunches by supervisors and the consumption of alcohol on duty, particularly within the Special Branch office where it seems a bar was regularly opened in the afternoon;

- the opening of dossiers and the keeping of records in respect of various persons, for example, barristers practising in the criminal law who on no reasonable basis could have been of interest to Special Branch within its charter;
- the ineffective and outdated intelligence system it maintained;
- the belief that it had long been associated with political interests, and seen as an agency which could be used for political advantage against persons on whom 'dirt files' had been kept;
- the limited investigative success it had achieved in relation to subversive activities in the past;
- the destruction of files soon after the Royal Commission was announced; and
- the unsatisfactory recruitment practices of the Branch which were based on patronage and friendship (Wood 1997, pp. 251-252).

Special Branch records were secured when the Branch was disbanded. The Police Integrity Commission subsequently undertook an investigation of these Special Branch holdings. In June 1998, the Commission tabled a report in Parliament regarding the outcomes of its investigation. One of the main criticisms of Special Branch was its lack of accountability and external scrutiny. The Commission's report included adverse comments regarding a number of Special Branch practices, including:

- a closed shop approach to recruitment, leading to cronyism and the perpetuation of outdated cultures and work practices
- a lack of accountability whereby the Mission Statement was updated, but no effective scrutiny of the Special Branch's activities was undertaken and no attempt was made to bring those activities in line with its changing charter
- information gathering on people who posed no threat of politically motivated violence or similar matters continued unabated, despite criticism of this practice by the Privacy Committee in 1978 and a recommendation for the implementation of guidelines to avoid it
- an unacceptable overlap between the functions of information gathering and protection of VIPs, leading to information being held about VIPs and public figures, rather than those who posed a threat to them
- minimal internal supervision of administrative activities, such as the creation and destruction of records, and what kind of information should be recorded
- the manual filing systems were anachronistic and unreliable, and
- no satisfactory procedures for the management and payment of informants (Police Integrity Commission 1998, pp. 29-30).

IDENTIFIED NEED FOR SAFEGUARDS AND OVERSIGHT FOR FUTURE UNITS

The Commissioner of Police and the Royal Commission each identified the need for a range of safeguards to be established for any unit that was to replace the Special Branch.

In its Final Report, the Royal Commission noted that the Commissioner of Police had foreshadowed the creation of a new agency, proposed to be called the 'Protective Security Response Group' (PSRG), to replace the Special Branch. Furthermore it listed the range of practices to safeguard the operation of this agency that were proposed by the Commissioner of Police, including:

- detailed integrity tests and vetting would be conducted of all members of the PSRG, who would be subject to a five-year tenure policy
- the PSRG would be answerable to the Deputy Commissioner of Special Operations, and intelligence collection and retention would be subject to sanctioning by a management committee chaired by the Deputy Commissioner Specialist Operations, and including the Commander PSRG and the Commander Olympic Security Group
- the Joint Audit team currently conducting the audit of Special Branch holdings would be consulted in the design of an ethical records management system
- all work would be properly assessed, prioritised and approved by a senior officer before allocation
- a 'job' database would be created to record all service requests and all information and action would similarly be recorded on the database
- the Service would consult with representatives of ASIO, Foreign Affairs, the AFP, and other groups in relation to records management and functions
- the PSRG would not control Informant Management funds
- there would be a random and external audit to ensure ethical target selection, collection, storage and use of intelligence
- a group operating manual and risk management guidelines would be developed (Commissioner of Police cited by Wood 1997, p. 253).

The Royal Commission supported the creation of the PSRG, or a similar body, subject to both the guidelines identified above as well as to an annual audit by the Deputy Commissioner of Special Operations, in conjunction with the Commissioner of the Police Integrity Commission, to ensure that:

- it is performing to its charter
- its staff are sufficiently aware of its mission statement and have not reverted to the practices of old
- it is adhering to strict controls on the use and payment of informants
- it has sound operating procedures, and that

- proper procedures exist for the recording and use of intelligence gathered (Wood 1997, p. 254).

In its report to Parliament in June 1998, the Police Integrity Commission recommended that the Royal Commission's proposal that a new, highly accountable agency to replace the former Special Branch 'be enacted as a priority' (Police Integrity Commission 1998, p. 33).

2.2 PROTECTIVE SECURITY GROUP

HISTORY AND ROLE

The PSG was established in August 1998 as the successor to the former Special Branch. The PSG's functions were subsequently subsumed into the newly created CTCC in March 2003.

The second reading speech for the *Police Legislation Amendment (Protective Security Group) Bill 1998* outlined the proposed role of the PSG. In this second reading speech, the Government acknowledged that the legitimate functions of Special Branch would need to be maintained. In introducing this legislation, Mr Whelan, the then Minister for Police, noted that after the abolition of the Special Branch an interim VIP security unit had been established. However, he stated that there remained a need for an agency with the broader capacity to:

- provide protective services and associated risk and threat assessments
- undertake operational and tactical analysis, intelligence gathering and liaison with relevant agencies in relation to persons who present a risk of politically-motivated violence or terrorism activity
- protect holders of high office in NSW, and
- coordinate investigations with other agencies tasked with preventing terrorism and politically-motivated violence.

Mr Whelan said that the Police Commissioner had proposed the establishment of the PSG to meet these needs (NSW Legislative Assembly, 23 June 1998, p. 6254).

The 'mission' of the PSG, as described in its charter, involved the protection of dignitaries as well as analysis, intelligence gathering and liaison in relation to politically motivated violence or terrorist activity:

> The PSG has the functions of:
>
> 2.1 Providing close personal protection for VIPs, internationally protected persons and other dignitaries and carrying out related intelligence gathering and risk/threat assessments.
>
> 2.2 Tactical/operational analysis, intelligence gathering and liaison with other relevant agencies, in relation to approved targets

> who present a risk of politically motivated violence or terrorist activity (NSW Police (undated), p. 1).

The description of the role of the PSG remained unchanged in NSW Police annual reports between 1999-2000 and 2001-2002:

> Protective Security Group provides close personal protection for VIPs, internationally protected persons and other dignitaries and carries out related intelligence gathering and risk/threat assessments (NSW Police 1999, pp. 35, 41; NSW Police 2000, p. 17; NSW Police 2001, p. 34; NSW Police 2002, p. 30).

Reflecting these functions, the PSG was comprised of two units:

- The VIP Protection Unit, which provided dignitary protection for the NSW Police Service, was staffed by 18 police officers, and
- The Counter Terrorist Intelligence Unit, which provided intelligence analysis and criminal investigations related to politically motivated violence, was staffed by 12 police officers (NSW Police Service 2000, pp. 3, 5).

The PSG was to undertake only those investigations of a minor nature. Any major incident was considered the responsibility of the Crime Agencies Command (NSW Police Service 2000, p. 8).

The functions of the PSG required it to 'continually liaise' with the AFP, ASIO, Protective Security Co-ordination Centre, Department of Foreign Affairs and Trade, and the NSW Consular Corps (NSW Police Service 2000, p. 4).

The PSG's charter limited those it could target and those on whom it could record information:

> The PSG shall not target or keep any records or file on any sensitive individual or group, as defined in section 14, without the approval of the PSG Management Committee, comprising the Deputy Commissioner Specialist Operations, Commander PSG, Commander Olympic Security Command Centre (until year 2000), Director State Intelligence Group. The Committee will report to the Commissioner of Police (NSW Police Service 2000, p. 7).

IDENTIFIED NEED FOR OVERSIGHT

As outlined in the previous section of this chapter, both the Commissioner of Police and the Royal Commission had identified the need for special safeguards and oversight requirements to be put in place for any agency replacing the former Special Branch.

Similarly, the NSW Government emphasised the need for special oversight for the PSG when introducing the *Police Legislation Amendment (Protective Security Group) Bill 1998.* In the second reading speech, Mr Whelan said that the Government endorsed the formation of the PSG, 'provided appropriate safeguards are put in place'. He elaborated:

> The Government remains of the view that any unit with these unusual functions should be subject to high standards, and an even higher level of scrutiny than most. The Protective Security Group will operate strictly according to a charter which sets out the roles and functions of the group. In addition the bill outlines strict accountability mechanisms relating to target selection, records and record management, and information dissemination.
>
> The bill provides that the charter of the group will be determined by the Commissioner of Police and approved by the Minister. The charter outlines the activities that the group is authorised to engage in, provides a formal mechanism for approval of targets to be investigated, sets out criteria for approval of targets, and sets strict limits on the keeping of records and files by the group. Strict adherence to the charter is a critical test for the proposed Protective Security Group. The Government is not prepared to leave this to chance and is putting in place a mechanism to ensure that the charter is adhered to (NSW Legislative Assembly, 23 June 1998, pp. 6254-5).

From the context, it would be reasonable to assume that when Mr Whelan spoke of 'any unit with these unusual functions', the types of functions that he would have been referring to were the 'legitimate functions of the former Special Branch', which he had previously described as including: 'capacity to provide protective services and associated risk and threat assessments, to undertake operational and tactical analysis, intelligence gathering and liaison with relevant agencies in relation to persons who present a risk of politically-motivated violence or terrorism activity, to protect holders of high office in this State and to coordinate investigations with other agencies tasked with preventing terrorism and politically-motivated violence' (NSW Legislative Assembly, 23 June 1998, p. 6254).

Furthermore, the Government was not convinced that NSW would continue to need an ongoing group with the functions of the PSG after the completion of the Sydney Olympic Games in 2000. For that reason, the NSW Government included in the legislation a requirement for a review of the need for such a unit following the Olympic Games:

> The bill will ensure that the Government is put in the best possible position to judge whether there is still a need for the Protective Security Group when our international visitors have returned home at the conclusion of the Olympics. It will ensure that the reconsideration of the role of the Protective Security Group is undertaken with external oversight and in an objective manner (NSW Legislative Assembly, 23 June 1998, p. 6255).

Mr Whelan concluded his introduction of this bill with the following summation:

> This bill puts into place the legislative framework for the oversight of the Protective Security Group which the Government considers to be an essential element in the establishment of the group. No branch of the Police Service will be under closer scrutiny than the Protective Security Group. As I have outlined, that scrutiny will include external monitoring by the PIC. By establishing the oversight mechanism outlined in this bill the Government is giving effect to the recommendations of the royal commission and the PIC and is acting to ensure the protection of citizens of this State from terrorist violence and from rogue police misusing their powers (NSW Legislative Assembly, 23 June 1998, p. 6256).

In response Mr Hartcher, the Member for Gosford, said that the Opposition supported the oversight mechanisms that were proposed:

> The Opposition … welcomes the fact that [the PSG] will be subject to guidelines and controls. … The Opposition is pleased to note that internal audits will be conducted in accordance with various stipulations laid down in the bill (NSW Legislative Assembly, 24 June 1998, p. 6449).

NATURE OF LEGISLATED OVERSIGHT REGIME

The *Police Legislation Amendment (Protective Security Group) Act 1998*, established the regime required to oversight the operation of the PSG. The Act amended both the *Police Act 1990* and the PIC Act.

Section 16 of the *Police Act 1990* was amended to require the Commissioner of Police to carry out an annual audit of the operations, policies and procedures of the PSG. These annual audits were required by the legislation to include an examination of:

- whether the Group as a whole is adhering to its charter and effectively performing its role as provided in its charter
- whether the members of the Group are adhering to its charter
- whether proper procedures exist and are being adhered to by the Group in connection with the use and payment of informants, and
- whether proper procedures exist and are being adhered to by the Group for the recording and use of intelligence gathered by the Group.

In addition to the annual audit, there was a requirement, under the new section 17 of the *Police Act 1990*, for the Commissioner of Police to cause a special review of the operations, policies and procedures of the PSG to be carried out as soon as practicable after the conclusion of the Sydney Olympic Games. This special review was to include an examination of whether the PSG has adhered to its charter and whether the group will have an effective role to perform in the future.

As an additional monitoring measure, section 14 of the PIC Act was amended to require the Commission to monitor and report on the conduct and effectiveness of the annual audits of the PSG, conducted by NSW Police (under section 14(e)). In addition the Commission was required to assess and report on the recommendations as to the future of the PSG contained in the special review of the PSG that was to be prepared following the conclusion of the Sydney Olympic Games (under section 14(f)).

It is important to note that there is no other business unit or command in NSW Police for which there is a specific statutory requirement for oversight by the Commission.

Annual audits of the PSG were carried out for the years 1998 to 2002 and were monitored by the Commission (Police Integrity Commission 2001, pp. 35-38; Police Integrity Commission 2002, pp. 35-36; Police Integrity Commission 2004, pp. 27-29).

2.3 COUNTER TERRORIST COORDINATION COMMAND - A NEW COMMAND INCORPORATING THE FUNCTIONS OF THE PROTECTIVE SECURITY GROUP

HISTORY AND ROLE

In October 2002 Mr Carr, the then Premier of NSW, announced the formation of the CTCC. He stated that Police Commissioner Moroney had completed the internal review of the NSW Police counter-terrorism capacity and reported to the then newly established Cabinet Sub-Committee on Counter Terrorism. Furthermore, Premier Carr said that the Cabinet had agreed that the CTCC would comprise 70 staff and be responsible for:

- public order management
- tactical response
- counter terrorist intelligence response
- critical infrastructure protection
- consequence management, and
- training (Premier of NSW 2002, p. 1).

When establishing the CTCC, the Cabinet had also approved:

- $5 million for bomb disposal and forensic services detections, inspection and containment equipment and the employment of chemists
- acquisition of an eight-seat Eurocopter BK 117 helicopter to transport bomb specialists, forensic analysts or State Protection Group teams to critical incidents at a cost of $4.8 million
- $1.9 million for officer protection, communication and transport for the State Protection Group
- $2.5 million for equipment and protective gear to combat biological, chemical and radiological threats, and
- $1.8 million for enhanced electronic surveillance (Premier of NSW 2002, p. 1).

The NSW Commissioner of Police was quoted as saying that the CTCC's most important task 'will be to make key tactical and strategic decisions based on intelligence' (Premier of NSW 2002, p. 2).

As mentioned previously, the CTCC was established in March 2003. When describing structural changes in its 2002-2003 Annual Report, NSW Police said that the CTCC:

> has been established, absorbing the Protective Security Group into an enhanced larger command to counter terrorism. … the CTCC mission is to provide a comprehensive and coordinated response to potential

> terrorist acts or politically motivated violence. The Command does this through intelligence analysis and investigation services and protection for dignitaries, national icons, business interests and critical infrastructure (NSW Police 2003, p. 18).

In its 2003-2004 Annual Report, NSW Police stated that as at 1 September 2003, NSW Police had adopted a new organisational structure which, amongst other changes, had involved bringing the CTCC, Protective Security Group and the State Protection Group (including Tactical Operations, Negotiators, Bomb Disposal and the Dog Unit) together under the command of the Assistant Commissioner Counter Terrorism (NSW Police 2004, pp. 10, 11). In this report, NSW Police described the role of the CTCC as follows:

> The Counter Terrorist Coordination Command provides intelligence gathering and investigation in relation to politically motivated violence, terrorist activity, public order management, dignitary protection, critical infrastructure protection, threats to high office holders, and threats to the diplomatic and consular corp. It also provides a tactical response through the services of the State Protection Group, including Tactical Operations, Negotiators, Bomb Disposal and Dog Unit (NSW Police 2004, p. 10).

Further information on the nature of the role, functions and structure of the CTCC can be found in Chapter 6 and subsequent chapters in this report where the information provided by NSW Police for this assessment is described.

The annual audits of the PSG that had been undertaken by NSW Police stopped when the CTCC was established.

OPERATIONAL CONTEXT

As NSW Police has observed in its 2004-2005 Annual Report, 'since the terrorist attacks on the World Trade Centre in 2001 and the Bali bombing in 2002, community attention has been focused on the potential for terrorist attacks here on our home soil' (NSW Police 2005, p. 28).

The NSW Government 2006-07 Budget provided an additional $1.8 million towards the maintenance of counter-terrorist activities. The narrative provided with the NSW Government 2006-07 Budget Estimates stated that the CTCC, working closely with other state, national and international agencies, has undertaken several high profile counter terrorism operations and investigations. Furthermore it stated that:

> An increasing emphasis will be given to engaging business and local communities in identifying and responding to potential terrorist threats, Closer ties will be developed with international jurisdictions to exchange intelligence and operational tactics (NSW Treasury Budget Estimates 2006, p. 16-5).

The $1.8 million that has been allocated for counter-terrorism activities includes the maintenance of a bomb disposal unit (Treasurer's Speech 2006-2007, p. 18).

2.4 PARLIAMENTARY COMMITTEE – TWO RELATED INQUIRIES

FEBRUARY 2004 INQUIRY

In February 2004, the Committee commenced an inquiry into the Commission's jurisdiction to oversight the PSG. The Terms of Reference specified that this was an inquiry into:

> a. the functions of the PIC under ss. 14(e)-(f) of the *Police Integrity Commission Act 1996*
>
> b. the provision of reports to the PIC under Part 3 of the *Police Act 1990*
>
> c. oversight of the conduct of NSW Police officers involved in the Counter Terrorism Coordination Command (CTCC), and
>
> d. any other matter that the Committee considers relevant to the inquiry (Parliament of NSW Committee on the Office of the Ombudsman and the Police Integrity Commission 2005, p. v).

The Chairman of the Committee, in his foreword to the Committee's interim report on this inquiry, remarked on the apparent inconsistency between the stringent oversight requirements legislated for the former PSG and the failure to specifically provide any specific oversight requirements for the new CTCC:

> While the Government was 'not prepared to leave … to chance' the oversight arrangements for the powers and functions of the PSG, it did not clearly provide for such oversight arrangements for the new CTCC, an organisation with more than double the budget, staff and resources of the PSG.
>
> Legislative clarification of this anomaly does not appear to be in sight. The review of the Police Act 1990, now more than two years overdue, would have provided an appropriate opportunity to deal with this issue. However, it appears that this opportunity has not been realised. As such the Committee resolved to conduct this inquiry (2005, p. vii).

The interim report of the inquiry further clarified that the purpose of this inquiry is to review the need for oversight for the CTCC and how any required oversight can best operate:

> This inquiry assesses the need for oversight of the CTCC as the body that has taken on, and substantially enhanced, the role of the PSG. The inquiry has been undertaken with a view to recommending how such oversight can best operate within the existing accountability regime. The inquiry will seek to establish a base level of appropriate oversight for the CTCC given that the CTCC has far greater resources and powers than the PSG (Parliament of NSW Committee on the Office of the Ombudsman and the Police Integrity Commission 2005, pp. 1-2).

In its interim report, the Committee observed that the amalgamation of the PSG into the CTCC had two outcomes: firstly, to increase the size, resources and powers of the unit and secondly, to reduce the oversight:

> The powers once possessed by the PSG have been greatly enhanced under the CTCC … Personnel, resourcing and powers have increased as Special Branch evolved into the PSG and then into the CTCC. … The second, and possibly unintended result has been that the Government's position that 'any unit with these unusual functions should be subject to high standards, and an even higher level of scrutiny than most' has been severely eroded (Parliament of NSW Committee on the Office of the Ombudsman and the Police Integrity Commission 2005, p. 33).

Furthermore, the Committee argued that 'given the expanded powers now held by the CTCC, the PIC's review of the NSW Police audit reports takes on added significance as an accountability measure' (p. 33).

As part of the Committee's inquiry, it posed a number of 'questions on notice' to the Commission. One of these questions sought the Commission's view on the need for oversight of the CTCC:

> Does the PIC feel there is any need to continue auditing the powers held by the PSG that are now held by the CTCC? (Parliament of NSW Committee on the Office of the Ombudsman and the Police Integrity Commission 2005, p. 41).

On 19 May 2004, the Commission responded to these questions on notice. In its response to this question, the Commission noted that:

- although the PSG no longer exists as a functional unit, there can be no doubt the 'unusual functions' previously performed by the PSG are now being performed by the CTCC
- the existing provisions in the *Police Act 1990* concerning the conduct of annual audits of the PSG and in the PIC Act concerning the monitoring of those audits do not apply to the CTCC
- legislative amendments would be required for the same auditing and monitoring processes to occur in relation to the CTCC
- as to whether or not these amendments are sought is a matter for Government
- legislating the type of oversight and the frequency with which it is to occur in connection with one functional area of NSW Police is restricting for both NSW Police and the Commission, providing little flexibility as to the roles played by each agency and the frequency of the audits; and problematic in so far as it is not supported by any ongoing assessment process examining the risk associated with the performance of the 'unusual functions' previously performed by the PSG, now by the CTCC
- the risks associated with functions performed by, or functional units within, police agencies may be subject to change over time
- it believed there would be some merit in evaluating the current level of risk through a structured process and, on that basis, determining the most appropriate risk treatment strategies to occur over a specified period of time, and

- the current absence of a legislative provision for auditing and monitoring the CTCC does not in anyway preclude the Commission from exercising its functions and powers in connection with the CTCC (Parliament of NSW Committee on the Office of the Ombudsman and the Police Integrity Commission 2005, pp. 41-43).

MARCH 2006 INQUIRY

On 29 March 2006, the Committee established a second, related inquiry into scrutiny of NSW Police counter-terrorism and other powers with the following terms of reference:

> a. the functions of the PIC and Ombudsman under the counter-terror laws of NSW and in relation to oversight of police use of covert and coercive powers
>
> b. oversight of the conduct of NSW Police officers involved in the Counter Terrorism Coordination Command
>
> c. trends in anti-terror laws and oversight of these extraordinary powers
>
> d. impact of the growth of police powers on the nature of external police oversight
>
> e. any other matter that the Committee considers relevant to the inquiry.

In correspondence from the Chairman for the Committee to the Commissioner of the Commission, this second inquiry was described as 'forming the final phase of the Committee's previous inquiry into the oversight of the Protective Security Group' (correspondence dated 30 March 2006).

THE COMMISSION'S SUBMISSION

In its written submission, dated 12 August 2004, to the first of the Committee's inquiries in this area, the Commission identified the need to develop a better understanding of the nature of the misconduct risks faced by those working in the CTCC:

> any position regarding future arrangements for the preventative audit/oversight of the CTCC, should be based on a clear understanding of the risks for police misconduct associated with its activities and structure (Parliament of NSW Committee on the Office of the Ombudsman and the Police Integrity Commission 2005, p. 38).

In its submission, the Commission expressed its understanding that the purpose of the PSG audit and monitoring regime was to maintain vigilance, as a preventative measure, in the face of special risks which were perceived to be associated with the 'unusual functions' of the PSG. As such, the primary goal of the Commission's proposed risk assessment was stated to be:

> to determine what special risks for police misconduct, or circumstances conducive to police misconduct, are associated with the actual and potential activities and structure of the CTCC or similar units.

The Committee accepted the Commission's proposal and concluded its interim report by stating that it would await the outcomes of the Commission's risk assessment before concluding its inquiries and tabling a final report (p. 38).

2.5 SUMMARY OF KEY POINTS

1. From the available documentation it seems that there are many similarities as well as some differences between the functions of the current CTCC and the functions of the former Special Branch and the former PSG. Like both the Special Branch and the PSG, the CTCC is responsible for providing intelligence concerning politically motivated violence, civil disorder, terrorist and extremist activity as well as providing protective services. Unlike the earlier units the CTCC also has responsibility for critical infrastructure protection and consequence management. The CTCC is also a larger unit with more resources than its predecessors.
2. There was no formalised provision for oversight of the former Special Branch which was identified as having major failings in the areas of:
    - disregard of its charter and a lack of accountability
    - information gathering on people who posed no threat of politically motivated violence or similar matters (inappropriate targeting) and the belief that it could be used for political advantage against persons on whom 'dirt files' had been kept
    - an unacceptable overlap between the functions of information gathering and protection of VIPs, leading to information being held about VIPs and public figures, rather than those who posed a threat to them
    - informant management and payment of informants
    - poor record keeping practices
    - ineffective and outdated intelligence system
    - poor supervision
    - unsatisfactory recruitment practices.
3. The former Commissioner of Police, the Royal Commission, and the NSW Government each identified the need for a range of safeguards as well as special oversight to be established for any unit that was to replace the Special Branch.
4. The oversight, formalised in legislation, for the PSG involved annual audits directed at specific aspects of the operation of the PSG and monitoring of these audits by the Commission.
5. There is no formalised provision for oversight of the CTCC.
6. The Committee has commenced an inquiry to consider whether or not a specific oversight regime is needed for the CTCC and, if such oversight is required, the form it should take.

3. LEGISLATIVE CHANGES IN THE AREA OF COUNTER-TERRORISM POLICING

One of the arguments for the CTCC to have a different oversight regime from that of other commands is that the officers of the CTCC have access to powers that are not available to other areas of NSW Police. The powers available to assist the policing of terrorism have increased with the introduction of new legislation and may continue to increase with any further changes in legislation.

This chapter outlines the nature of the powers and accountability mechanisms that have resulted from legislative changes in counter-terrorism policing. Following some initial background concerning the referral of terrorism powers to the Commonwealth, this chapter focuses on NSW legislation enacted since late 2002. (Further information about the object of each of the pieces of NSW legislation, the police powers and limitations of these powers, and the authorisation process and accountability requirements provided within the legislation can be found in Appendix 3.)

3.1 REFERRAL OF TERRORISM POWERS TO THE COMMONWEALTH

As Justice McClellan[1] (2006) has observed, prior to 11 September 2001 the Northern Territory was the only Australian jurisdiction to have enacted specific terrorist offences (p. 6). In 2002, the Australian parliament passed legislation which introduced crimes of 'terrorism' for the first time in federal law (Hocking 2003, p. 1).

A summit of Commonwealth and State and Territory leaders (Leaders' Summit on Transnational Crime and Terrorism), held in Canberra on 5 April 2002, resulted in State governments referring their powers over terrorism to the Commonwealth. The Commonwealth *Criminal Code Amendment (Terrorism) Act 2003* provides for the Commonwealth to legislate in this area. At the State level, NSW introduced the *Terrorism (Commonwealth Powers) Act 2002* in December 2002 to refer certain matters relating to terrorist acts to the Commonwealth Parliament in accordance with section 51 (xxxvii) of the Commonwealth Constitution, to enable the Commonwealth Parliament to make laws about these matters.

As stated in the National Counter-Terrorism Plan, Australia maintains a 'national, cooperative approach to counter-terrorism':

> The nature of terrorism means that its implications may cross jurisdictional boundaries. This, and the range of preventive measures and capabilities that may be required, necessitates that Australia maintain a national, cooperative approach to counter terrorism. Coordination and consultation between jurisdictions is formalised by the Inter-governmental Agreement on Australia's National Counter-Terrorism Arrangements of 24 October 2002 (National Counter-Terrorism Committee 2005, p. 2.2).

[1] Chief Judge at Common Law in the NSW Supreme Court.

As a result, while many laws have been enacted to combat terrorism at the Commonwealth level (see, for example, McClellan 2006, p. 35), there is relatively little State or Territory legislation relating to counter-terrorism.

The NSW counter-terrorism legislation which specifically affects police powers is the *Terrorism (Police Powers) Act 2002* and its subsequent amendments:

- *Crimes Legislation Amendment (Terrorism) Act 2004*
- *Terrorism Legislation Amendment (Warrants) Act 2005*
- *Terrorism Legislation Amendment (Preventative Detention) Act 2005*.

3.2 IDENTIFIED NEED TO BALANCE POWERS WITH ACCOUNTABILITY

When introducing the *Terrorism (Police Powers) Act 2002* and its subsequent amendments, the NSW Government has emphasised the need to balance police powers with accountability measures and safeguards. For example, when introducing the *Terrorism (Police Powers) Bill* in November 2002 the former Premier, Mr Carr, described both the limitations to the circumstances in which the powers can be used as well as the needs for checks and balances:

> The new powers given to police are confined to limited circumstances. As I have said repeatedly, it is not my instinct to fling at police and security agencies crudely increased powers. In any democracy there must be a healthy suspicion of law enforcement powers. We must carefully monitor their use. We have time-limited the increased powers and created a special trigger before they can be invoked. That is an alternative model to just saying that police shall have these extra powers to search, and to do so in all these circumstances.
>
> We are not doing that. We are saying that where there is a credible terrorist threat, or where there has been an actual incident, for a period of seven days and two days respectively police will enjoy these increased powers. Then the powers automatically lift unless they are specifically renewed. That is a time limit on these powers. It is a check. It is a balance. Moreover, we are making sure that in these areas – as in all areas – the police and their behaviour are subjected to the oversight of the Police Integrity Commission and the Ombudsman. So there will be that review capacity, as there ought to be. We want accountability to apply even where police are responding to terrorism (NSW Legislative Assembly Hansard, 19 November 2002).

Similarly when introducing the *Terrorism Legislation Amendment (Warrants) Bill 2005*, Mr Bob Debus (Attorney General and Minister for the Environment) discussed the need for safeguards:

> These powers [covert search warrants] are extraordinary and will be permitted only with the strictest of safeguards, including the following. Warrants may be issued only when there is reasonable suspicion or belief that a terrorist act has been, is being, or is likely to be committed. Annual reports must be made to the Attorney General and the Minister of Police regarding the exercise of these powers. Any complaint regarding the exercise of these powers can be investigated by the established

> bodies, the NSW Ombudsman, the Commissioner of Police and, where appropriate, the Police Integrity Commission. The scheme will be kept under constant legislative review through the existing review provisions in the Terrorism (Police Powers) Act, which requires yearly reports. The scheme is subject to independent monitoring by the Ombudsman for a period of two years.
>
> Those safeguards are an attempt to balance the legitimate needs of law enforcement and the right of privacy that citizens enjoy (NSW Legislative Assembly 2005, p. 16940).

In response to debate on this legislation, Mr Debus once again emphasised the safeguards incorporated in this legislation:

> I emphasise in this context that these powers [Terrorism Legislation Amendment (Warrants) Bill] have nothing to do with secret policing. Secret policing involves the exercise of powers by police without independent oversight, without accountability … The Government has gone to great lengths to ensure that the bill contains strong and robust safeguards in relation to the granting of these covert search warrants and their execution, and in the requirement that an occupier must ultimately be notified that a search has taken place (NSW Legislative Assembly 2005, p. 16944).

Additional extracts concerning accountability and oversight issues raised in the second reading speech and parliamentary debates associated with the introduction of this legislation are provided in Appendix 3.

3.3 POWERS PROVIDED BY NSW LEGISLATION

Police powers have been provided to assist in the prevention of a terrorist attack occurring in the near future or to assist in apprehending the person(s) responsible for a terrorist attack that has occurred. These powers are not restricted to officers employed in the CTCC. Following authorisation, many of these powers are available to be used by any NSW Police officer.

The police powers that are provided by the *Terrorism (Police Powers) Act 2002* and its subsequent amendments are summarised in Table 3.1. From this table it can be seen that, under specified circumstances, NSW Police officers have been provided with additional powers to:

- obtain a disclosure of identity (section 16)
- stop and search a person (without a search warrant) (section 17)
- stop and search vehicles (without a search warrant) (section 18)
- enter and search premises (without a search warrant) (section 19)
- seize and detain things (section 20)
- use reasonable force (section 21)
- give directions to government agencies for the purpose of exercising police special powers under the Terrorism (Police Powers) Act 2002 (section 14A)

- place a cordon around a target area (section19A), and
- allow a person to be taken into custody and detained for a short period of time to prevent an imminent terrorist act, or to preserve evidence of, or relating to, a recent terrorist attack (Part 2A).

In addition, 'eligible officers' (that is, an officer employed in a NSW Police group designated as the 'terrorism investigation group' by the Commissioner of Police or an eligible member of the Crime Commission) may enter, without any occupier's knowledge, and search premises under the authority of a special covert search warrant (section 27O).

3.4 AUTHORISATION AND ACCOUNTABILITY REQUIREMENTS INCORPORATED IN NSW LEGISLATION

Table 3.1 also summarises the authorisation process and the accountability requirements incorporated in the NSW legislation.

AUTHORISATION

The level of officer who can apply to use different powers and who can authorise their use differs amongst the different powers. For example, the powers to search a person, vehicle or premises (without a warrant) can be authorised by the Commissioner of Police or by a Deputy Commissioner of Police. If they cannot be contacted, authorisation can be given by any officer above the rank of superintendent. Concurrence of the Minister of Police is required unless he or she is not able to be contacted.

In relation to covert search warrants, approval of the Commissioner of Police or other senior officer of NSW Police (no more than two persons may hold this delegation at the same time) is required to apply for the issue of such a warrant. The warrant can be authorised only by an 'eligible judge'.

Similarly the list of those who can give approval for an officer to make an application for a preventative detention order is restricted (to the Commissioner of Police, a Deputy Commissioner or an Assistant Commissioner responsible for counter-terrorism operations). Only the Supreme Court can actually grant such an order.

ACCOUNTABILITY REQUIREMENTS

The accountability requirements provided in the legislation include appropriate documentation, reports on the use of the powers to the Attorney General and the Minister of Police and an annual review of the Act. The range of specific accountability requirements include:

- appropriate documentation of the authorisation describing the general nature of the terrorist act to which it is applied, name or description of the person, vehicle or area targeted and specifying the time that the authorisation ceases to have effect (section 10)
- provision of information, if requested by the person who is the subject of the police power (section 23)

- documentation by an eligible judge of all relevant particulars of the grounds he or she has used to justify or refuse the issue of a covert search warrant (section 27L)
- a report on the authorisation to the Attorney General and Police Minister as soon as practicable after the expiry of an authorisation (section 14B)
- a report must be made about the execution of a covert search warrant, by the person to whom a covert search warrant was issued, to the judge who issued the warrant (section 27S)
- annual reports of the exercise of powers relating to covert search warrants (section 27ZB) and preventative detention (section 26ZN) are to be made to the Attorney General and Minister for Police
- the covert search warrants aspect of the legislation is subject to independent monitoring with the NSW Ombudsman for a period of two years while the preventative detention aspects of the legislation is subject to independent monitoring by the NSW Ombudsman for five years
- a person who is held under a preventative detention order is entitled to contact the Ombudsman or the Commission (section 26ZF) - however, it is not clear that a detainee must be informed of this entitlement to contact the Commission, given that the Commission is conspicuous by its absence from section 26Y (2) which lists the nature of the information that must be provided to the detainee
- an annual Ministerial review of the Act to determine whether the policy objectives of the Act remain valid and whether the terms of the Act remain appropriate for securing those objectives. A report of the outcome of each of the annual reviews is to be tabled in Parliament (section 36).

Some of these accountability requirements (such as the documentation of the authorisation, documentation of the relevant particulars by the eligible judge, the report on the authorisation to the Attorney General and Police Minister, and the report to the judge concerning the execution of a covert search warrant) would occur at the time of authorisation or soon after the execution of the power and would be available to only a small number of people. Insufficient time has passed for the independent monitoring by the Ombudsman to have occurred and reports to be available in relation to the amendment made to the *Terrorism (Police Powers) Act 2002* by the *Terrorism Legislation Amendment (Warrants) Act 2005* or the *Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005* as these Acts were only introduced in late 2005.

The only one of these accountability requirements that potentially may have been publicly available was the annual Ministerial review of the *Terrorism (Police Powers) Act 2002*, which is required under section 36. This review is to be undertaken by the Attorney General, as the Minister who administers the Act. When the Commission enquired with the NSW Attorney General's Department in mid-July 2006, it was told that the first annual review of this legislation had been conducted and would soon be tabled in Parliament.

Table 3.1: Summary of police powers and accountability requirements provided by the *Terrorism (Police Powers) Act 2002* and associated amendments

Legislation	Terrorism (Police Powers) Act 2002 (as at December 2002)	Crimes Legislation Amendment (Terrorism) Act 2004 Schedule 3	Terrorism Legislation Amendment (Warrants) Act 2005	Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005
Date commenced	13 December 2002	6 July 2004	13 September 2005	16 December 2005
Powers	• To obtain disclosure of identity (s. 16) • To search person (s. 17) • To search vehicles (s. 18) • To enter and search premises (s. 19) • To seize and detain things (s. 20) • To use reasonable force (s. 21)	• To give directions to government agencies for the purpose of exercising police special powers under the *Terrorism (Police Power) Act 2002* (s. 14A) • To place a cordon around target area (s. 19A)	• To enter, without any occupier's knowledge, and search premises under the authority of a special covert search warrant (s. 27O).	• To allow a person to be taken into custody and detained for a short period of time to prevent an imminent terrorist act or to preserve evidence of, or relating to, a recent terrorist act (s. 26A).
Conditions under which powers can be used	Police officer giving authorisation needs to be satisfied that there are reasonable grounds for believing that: • there is an imminent threat of a terrorist act and that the exercise of the powers will substantially assist in preventing the terrorist act (s. 5), or • a terrorist act has been committed and that the exercise of the powers will substantially assist in apprehending the persons responsible for committing the terrorist act (s. 6)	Amended s. 5 so that it refers to a threat of a terrorist act occurring 'in the near future', rather than to an 'imminent' threat. Hence following this amendment police officer giving authorisation needs to be satisfied that there are reasonable grounds for believing that: • there is a threat of a terrorist act occurring in the near future and that the exercise of the powers will substantially assist in preventing the terrorist act (s. 5), or • a terrorist act has been committed and that the	The person giving the authorisation suspects: • that a terrorist act has been, is being, or is likely to be committed, and • that the entry to and search of premises will substantially assist in responding to or preventing the terrorist act, and • that it is necessary for the entry and search of those premises to be conducted without the knowledge of any occupier of the premises (s. 27C).	When there are reasonable grounds to suspect that the person: • will engage in a terrorist act, or • possesses a thing that is connected with the preparation for, or engagement in a terrorist act, or • has done an act in preparation for, or planning a terrorist act, and • making the order would substantially assist in preventing a terrorist act occurring, and

Legislation	Terrorism (Police Powers) Act 2002 (as at December 2002)	Crimes Legislation Amendment (Terrorism) Act 2004 Schedule 3	Terrorism Legislation Amendment (Warrants) Act 2005	Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005
		exercise of the powers will substantially assist in apprehending the persons responsible for committing the terrorist act (s. 6).		• detaining the person is reasonably necessary for the purpose of substantially assisting in preventing a terrorist act from occurring sometime in the next 14 days OR • a terrorist act has occurred in the last 28 days and it is necessary to detain the person to preserve evidence (s. 26D).
Who authorises use of power	Commissioner of Police or a Deputy Commissioner of Police. However, if not able to be contacted authorisation can be given by any officer above the rank of superintendent (s. 8). Concurrence of Police Minister required unless he or she is not able to be contacted (s. 9).	Unchanged	Approval to apply for a covert search warrant can be given by the Commissioner of Police or someone at or above the rank of superintendent to whom authority has been delegated (no more than 2 persons may hold delegations under this section at the same time) (ss. 27D & 27E). Eligible judges – Supreme Court judge who consents to be and who is nominated by the Attorney General (s. 27B) – can issue a covert search warrant (s. 27K).	Approval to apply for a preventative detention order can be given by the Commissioner of Police, a Deputy Commissioner of Police, or an Assistant Commissioner of Police responsible for counter-terrorism operations (s. 26F). Supreme Court can make an order or an interim order (ss. 26H and 26I).

Legislation	Terrorism (Police Powers) Act 2002 (as at December 2002)	Crimes Legislation Amendment (Terrorism) Act 2004 Schedule 3	Terrorism Legislation Amendment (Warrants) Act 2005	Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005
Who can employ power	Any NSW Police officer (s. 14(1)) and 'recognised law enforcement officers' including members of the AFP and members of the police force of another State or Territory (ss. 24 & 25).	Unchanged	'Eligible police officer' – i.e. one employed in NSW Police group designated as the 'terrorism investigation group' by the Commissioner of Police (or an eligible staff member of the Crime Commission) (s. 27A).	Any police officer (s. 26Q) who is to be oversighted by a police officer of or above the rank of superintendent (s. 26R).
Accountability requirements	• An authorisation must specify that it is made under the Act, describe the general nature of the terrorist act to which it applied, name or describe the person, vehicle or area targeted and specify the time that the authorisation ceases to have effect (s. 10). • If requested to do so, a police officer must provide certain information (e.g. that the officer is a police officer, his or her name and place of duty, and reason for the exercise of power) to the person subject to the exercise of a special power (s. 23). This is qualified by 'as soon as reasonably practicable after exercising the power'. • Commissioner of Police must provide a report on the authorisation to the Attorney General and the Police Minister as soon as practicable after the	Unchanged	• Eligible judge must cause a record to be made of all relevant particulars of the grounds that he/she has used to justify or refuse the issue of the warrant (s. 27L). • A person to whom a covert search warrant was issued must report back to the judge who issued the warrant about the execution of the warrant within 10 days after it was issued or after it expired (s. 27S). • Annual reports must be made to the Attorney General and the Minister for Police regarding the exercise of these powers (s. 27ZB). • The scheme is subject to independent monitoring by the NSW Ombudsman for a period of 2 years (s. 27ZC).	• The detained person is to be given a copy of the order and a summary of the grounds on which it is made (s. 26ZB). • The person being detained is entitled to contact the Ombudsman or the Police Integrity Commission (s. 26ZF). (While s. 26Y (2) specifies that the detainee must be notified of his/her right to complain to the Ombudsman, contact a lawyer, contact a family member or person he/she lives with, there is no specific requirement within the Act for the detainee to be notified of his right to contact the Commission.) • Annual reports must be made to the Attorney General and the Minister for Police regarding the

Legislation	Terrorism (Police Powers) Act 2002 (as at December 2002)	Crimes Legislation Amendment (Terrorism) Act 2004 Schedule 3	Terrorism Legislation Amendment (Warrants) Act 2005	Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005
	expiry of an authorisation (s. 26, subsequently renumbered as s. 14B). (However, it should be noted that an authorisation may not be challenged, reviewed, quashed or called into question by anything other than an investigation under the PIC Act (s. 13) and a police officer cannot be convicted or held responsible because there was a defect in giving the authorisation or the person who gave the authorisation lacked the jurisdiction to do so (s. 29).) • A Ministerial review of the Act is to be undertaken 12 months after the date of assent and every 12 months thereafter to determine whether the policy objectives of the Act remain valid and whether the terms of the Act remain appropriate for securing those objectives. A report of the outcome of each review is to be tabled in Parliament (s. 36).			exercise of these powers (s. 26ZN). • The scheme is subject to independent monitoring by the NSW Ombudsman for a period of 5 years (s. 26ZO). • The Commissioner of Police is to ensure that the Ombudsman is notified of the making of a preventative detention order, if a person is taken into custody under a preventative detention order, and of the revocation of such an order (s. 26ZO).

3.5 SUMMARY OF KEY POINTS

1. The counter-terrorism police powers are not confined to officers employed in the CTCC. With the exception of the powers concerning covert search warrants, the other police powers provided in the *Terrorism (Police Powers) Act 2002* can be employed by any NSW Police officer, though the use of these powers needs to be authorised. That authorisation can be given by only a relatively small number of individuals and can only be triggered under quite specific circumstances.
2. As a result of the covert nature of some of the powers, in many cases few people - other than the person who authorised the use of powers, the Minister for Police, the Attorney General and the officers using these powers - will be aware that the powers have been used. Hence, unlike some other police powers, the use of these powers is unlikely to be open to public scrutiny.
3. When introducing the *Terrorism (Police Powers) Act 2002*, and its subsequent amendments, the NSW Government has emphasised the need to balance police powers with accountability measures. Several accountability mechanisms were introduced as part of the legislation. However, their effectiveness, particularly in relation to minimising opportunities for officer misconduct, is yet to be tested.

4. MISCONDUCT RISK ASSESSMENT

This chapter provides a description of what the Commission means by 'misconduct risk'. It also describes the process the Commission followed to conduct this assessment of the management of the misconduct risks that arise from the nature of the work undertaken by officers in the CTCC.

4.1 MISCONDUCT RISKS

A misconduct risk is an organisational vulnerability for an employee to engage in corruption, fraud or some other form of misconduct. The types of misconduct risks faced by any employee depend on the nature of the work he or she undertakes.

Within policing, misconduct risks will vary according to the different types of functions carried out by police officers. For example, it is likely that the misconduct risks confronting a highway patrol officer would be quite different from those confronting an officer who handles drug exhibits. The work of highway patrol officers may, for example, bring these officers in contact with motorists who may offer them cash or some other inducement, to avoid a fine or other penalty. Officers who handle drug exhibits, on the other hand, may come into contact with exhibits that could fetch a significant amount of money if stolen and sold illegally.

Not all misconduct risks are equal. Misconduct risks differ in their likelihood of occurring and in their consequences if they were to occur. Although the nature of the misconduct risks likely to be encountered differ in terms of the work being done, there is no suggestion that an officer doing one type of work would be more prone to engaging in misconduct than another officer doing a different type of work. What is important is to identify the misconduct risks and how they best might be managed. Also, a greater number of risks does not necessarily result in more misconduct occurring: it all depends on how the risks are managed.

Misconduct risk management focuses on prevention activities. Misconduct risk management involves identifying, assessing, treating and monitoring the potential for future misconduct, rather than the management of individual officers who have been identified as having engaged in misconduct in the past. Misconduct risks are of interest because they present possible points to focus strategies to minimise future misconduct. One of the most valuable strategies to minimise future misconduct is to educate staff. Equipped with a good understanding of the nature of the work-related misconduct risks, it is possible to provide employees with the skills to recognise the misconduct risks that might confront them and the knowledge of how best to respond to such situations if they were to arise. Other useful strategies to minimise future misconduct involve reducing the opportunity or the motivation for misconduct to occur, making it more difficult to undertake, or increasing the likelihood of detection.

4.2 HOW THE COMMISSION UNDERTOOK THIS ASSESSMENT

The Commission consulted with senior levels of NSW Police and senior levels of the CTCC to discuss the reasons for conducting this assessment and the methodology proposed. The Commission formally and separately sought NSW Police corporate-

level views[2] and CTCC command-level views[3] on topics of interest, in addition to interviewing key staff of the CTCC.

The Commission also consulted more widely. This included:

- contacting a number of law enforcement agencies in regard to the management of the risk of misconduct in those areas tasked with similar responsibilities and with similar powers as the CTCC
- enquiring with the NSW Audit Office and with Treasury concerning risk management methodologies, and
- liaising with selected Australian and international researchers to identify available research on the relationship between misconduct risks and different police functions and powers as well as to identify available research on risk management in policing.

OBJECTIVES OF THE ASSESSMENT

As discussed in Section 1.3 in Chapter 1 of this report, the Commission conducted this assessment to develop a better understanding of:

1. What are the misconduct risks associated with the functions of the CTCC?, and
2. How well is NSW Police identifying, assessing and managing misconduct risks faced by those working in the CTCC?

INFORMATION COLLECTED

The Commission sought to answer these two broad questions by collecting information about four main areas:

- the strategies used corporately by NSW Police and at the command-level by the CTCC to identify, to assess and to decide how to treat risks in general, and misconduct risks in particular (see Chapter 5 for a description of the information collected)
- the nature of the work undertaken by the CTCC and the misconduct risks associated with this work (see Chapter 6 for further information)
- the strategies used to treat (manage or mitigate) the misconduct risks faced by officers working in the CTCC (see Chapter 7), and
- oversight arrangements currently in place and opinions about the most appropriate oversight arrangements for the future (see Chapter 8).

The Commission used a diverse and complementary range of sources to gather relevant information for this assessment of the management of the misconduct risks

[2] The Commission wrote to the Deputy Commissioner of Specialist Operations to obtain NSW Police 'corporate-level views'.

[3] The Commission wrote to the Assistant Commissioner Counter Terrorism to obtain the CTCC 'command-level views'.

that arise from the nature of the work undertaken by officers in the CTCC. These sources included:

- corporate-level responses provided by NSW Police to written questions from the Commission
- command-level responses provided by the CTCC to written questions from the Commission
- structured face-to-face interviews conducted with key staff of the CTCC and the Public Order Riot Squad (PORS) - including both officers who held the position of Assistant Commissioner Counter Terrorism and Public Order Management during the period the Commission was collecting its information, the Commander of the CTCC, the team leaders or acting team leaders of the units within the CTCC and the Commander of PORS - during March-April 2006 (these officers were generous with their time and their responses, with each interview lasting between two and three hours)
- published literature to identify possible misconduct risks faced by officers working in the CTCC based on:
  - the criticisms of the former Special Branch previously raised by the Royal Commission and by the Police Integrity Commission
  - any available information relating types of police misconduct to different police functions and powers
  - relevant inquiries such as the report of the Senate inquiry into new terrorism laws, relevant submissions to that inquiry, and the Wheeler review into airport security and policing
- legislation to identify new counter-terrorism policing powers and accountability measures incorporated in the legislation
- available prosecutions on terrorism suspects for any comments made about NSW Police investigations in these prosecutions
- complaints made about officers assigned to the CTCC, and
- relevant NSW Police policies and other documentation.

Table 4.1 itemises the topics examined in relation to the four main areas of interest from each of the different information sources.

In order to verify the accuracy of the Commission's description of NSW Police and CTCC misconduct risk management strategies, and in keeping with the consultative approach in which it had been conducted, prior to finalising this assessment the Commission referred a copy of a draft of its report to NSW Police in mid-August 2006. After receiving NSW Police feedback in a meeting on 20 September 2006, the Commission finalised its assessment.

LIMITATIONS OF THE ASSESSMENT

The project did not encompass:

- NSW Police business units or commands that did not fall under the control of the Assistant Commissioner Counter Terrorism
- risks other than misconduct risks, such as operational risks or financial risks
- the collection of information on persons or groups under surveillance and/or investigation by the CTCC or its liaison partners
- the examination of classified or sensitive documentation pertaining to groups or individuals of interest to the CTCC, or
- matters that would be caught in a standard financial audit.

While the primary focus was on the CTCC, at the suggestion of one of the Assistant Commissioners interviewed, information was also collected about the (at that time) recently-established PORS. The Commander of PORS was also included in the sample of officers interviewed for this project.

The information collected for this project primarily relies on the material provided by NSW Police. Where possible, supplementary sources (such as the review of past complaints made about CTCC officers, review of the relevant literature to identify potential misconduct risks and examination of minutes of meetings) were used to check and provide context to the information supplied by NSW Police. However, no attempt was made to view CTCC information holdings or to observe CTCC officers using their powers in any operations. Hence, this assessment is largely based on an examination of CTCC stated practices in the absence of any verification of how these practices are applied in the field.

4.3 SUMMARY OF KEY POINTS

1. The nature of the work that an employee undertakes affects both the range as well as the type of misconduct risks that an employee is likely to encounter.
2. Misconduct risk management focuses on prevention activities by identifying, assessing, treating and monitoring the misconduct risks that may be faced by an employee in the course of his or her work.
3. The Commission used a diverse range of sources to collect information on:
   - the strategies used by NSW Police and by the CTCC to identify, to assess and to decide how to treat risks in general, and misconduct risks in particular
   - the nature of the work undertaken by the CTCC and misconduct risks associated with this work
   - the strategies used to treat the misconduct risks faced by officers working in the CTCC
   - the oversight arrangements currently in place and opinions about the most appropriate oversight arrangements for the future.

Table 4.1: Summary of topics examined for this misconduct risk management assessment from different information sources

Information source	Information examined to understand and assess corporate and command-level misconduct risk management strategies	Information examined to identify potential misconduct risks facing the CTCC	Information examined to understand treatment strategies used to mitigate these misconduct risks	Information examined to determine current oversight regime and preferred options for future oversight
Written request for NSW Police corporate-level information	• NSW Police service-wide process for identifying, documenting, assessing, and managing risks • Statements or directions concerning command responsibilities for misconduct risk management • Resources provided to assist commands in the process of identifying, assessing and managing misconduct risks • Any monitoring of the effectiveness of the misconduct risk treatment strategies	• Current role and functions of the CTCC • Changes in structure, charter, roles and functions performed by successive units that have replaced the Special Branch • Whether the CTCC is seen as a command for which special misconduct risks exist due to its functions • Identification and documentation of misconduct risks facing CTCC officers	• Information or training provided by NSW Police about the misconduct risks officers are likely to face in their work and how best to manage these risks	• Areas of NSW Police that have been assigned responsibility for oversighting misconduct risk management across the organisation as a whole or within individual commands • Any monitoring of the effectiveness of the misconduct risk treatment strategies
Written request for CTCC command-level information	• CTCC process for misconduct risk identification, assessment and management • Resources available to assist the CTCC identify and manage misconduct risks within the command • Strategies to review the misconduct risks faced by officers working in the CTCC	• Current role and functions of the CTCC • Major functional areas of the CTCC • Misconduct risks identified as potentially being faced by CTCC officers • Assessment of these misconduct risks	• Strategies in place to reduce or manage each of the misconduct risks • Strategies in place to minimise practices previously criticised in relation to the operations of the former Special Branch, e.g., Mechanisms to ensure that the CTCC does not	

Information source	Information examined to understand and assess corporate and command-level misconduct risk management strategies	Information examined to identify potential misconduct risks facing the CTCC	Information examined to understand treatment strategies used to mitigate these misconduct risks	Information examined to determine current oversight regime and preferred options for future oversight
	or to review the risk reduction/ management strategies • Whether the CTCC monitors the effectiveness of the risk treatment strategies		disregard its charter; mechanisms to ensure that the work of the CTCC is accountable; mechanisms to ensure ethical target selection, collection storage and use of information • Any misconduct prevention strategies that are specific to the CTCC • Information provided to CTCC staff about the misconduct risks they are likely to face and how best to manage these risks	
Responses to structured face-to-face interviews conducted with key CTCC and PORS staff	• Processes used within the CTCC to identify and/or determine strategies to minimise or otherwise respond to misconduct risks • Documentation of these processes • Need for more training or assistance to identify misconduct risks or develop and implement strategies to manage misconduct risks that may be faced by their staff • Review of the misconduct	• Nature of the work carried out by the CTCC, different units within the CTCC, and by PORS • Misconduct risks faced by officers working within CTCC or PORS • Which risks do they consider most in need of attention • Possible emerging misconduct risks e.g. that might result from new legislation • Misconduct risks associated with covert search warrants	• Strategies in place to reduce or manage each misconduct risk • Views on other ways to reduce or manage each misconduct risk • Information provided to staff about misconduct risks within the CTCC • Strategies in place to minimise practices criticised in relation to the operations of the former Special Branch, e.g., mechanisms to	• Monitoring processes or systems in place to examine the effectiveness of the strategies used to manage misconduct risks • Any regular checks on the operations, policies and procedures of the CTCC by another area of NSW Police such as the audit group • Perceived benefits and perceived disadvantages of annual audit conducted on

Information source	Information examined to understand and assess corporate and command-level misconduct risk management strategies	Information examined to identify potential misconduct risks facing the CTCC	Information examined to understand treatment strategies used to mitigate these misconduct risks	Information examined to determine current oversight regime and preferred options for future oversight
	risks faced by officers working in the CTCC or of the risk reduction/management strategies • Suggested improvements for the process		avoid similar problems resulting from its recruitment practices; informant management and payment of informants • Mechanisms to avoid inappropriate targeting of individuals • Mechanisms regarding the appropriate collection, storage and use of information • How staff of the command keep up with legislative changes and how such changes affect their work • Suggestions for improvement	the PSG • Perceived benefits and perceived disadvantages of the external oversight such as that provided by the PIC oversight of NSW Police audits of the PSG • Views on what, if any, external monitoring or oversight arrangements are required to adequately manage misconduct risks faced by those who work in the CTCC • Suggestions for improvements to the current checks by NSW Police on the operations, policies and procedures of the CTCC
Examination of legislative provisions re counter-terrorism police powers		• Identify police powers provided under the legislation which officers can employ and the circumstances when officers can employ these powers	• Identify accountability measures provided under the legislation	

Information source	Information examined to understand and assess corporate and command-level misconduct risk management strategies	Information examined to identify potential misconduct risks facing the CTCC	Information examined to understand treatment strategies used to mitigate these misconduct risks	Information examined to determine current oversight regime and preferred options for future oversight
Literature review	• Identify risk management standards and guidelines available to NSW Police • Research conducted on risk management in other law enforcement agencies	• Types of misconduct identified by the Royal Commission and a Commission inquiry (Operation Brass) as occurring in the former Special Branch • Review of police misconduct literature that links between different policing functions with types of misconduct • Possible risks identified from the report of the Senate Inquiry into the new terrorist laws and relevant submissions to that inquiry and from the Wheeler review (Wheeler 2005)		
Review of complaints made against officers working in the CTCC		• identify misconduct allegation types to see whether these allegation types are similar to or different from allegations made about officers undertaking other types of police work • Are any of the allegations made about CTCC officers consistent with types of misconduct previously identified by the Royal		

Information source	Information examined to understand and assess corporate and command-level misconduct risk management strategies	Information examined to identify potential misconduct risks facing the CTCC	Information examined to understand treatment strategies used to mitigate these misconduct risks	Information examined to determine current oversight regime and preferred options for future oversight
		Commission in relation to the former Special Branch		
Consult interstate, federal and overseas agencies with counter-terrorist functions	Risk management strategies used	• Misconduct risks identified by other agencies		
Comments made about NSW Police investigations in available prosecutions of terrorism suspects		• Misconduct risks identified from comments on the NSW Police investigation of Zaky Mallah		
Documents examined	• CTCC CMF templates • Minutes of the CMT meetings to see whether the minutes reflect the use of these meetings to identify misconduct risks	• Minutes of the CMT meetings	• CTCC CMF templates • Standard Operating Procedures for Covert Search Warrants • CTCC information collection plan • CTCC induction materials for new staff	

5. RISK MANAGEMENT

This chapter provides a description of the processes that NSW Police in its corporate-level response and the CTCC in its command-level response advise are used to identify, analyse, evaluate, treat, monitor and communicate risks (in general), as well as misconduct risks (in particular).

To provide a context in which to consider these processes, this chapter commences with the results of two literature reviews that the Commission conducted to provide some baseline against which to assess the processes used by NSW Police. In the first of these, the Commission examined the guidelines available regarding risk management (in general) and misconduct risk management (in particular) to agencies such as NSW Police. In the second, the Commission examined available research on the use of risk management and misconduct risk management within other law enforcement agencies.

5.1 PROVIDING SOME CONTEXT

RISK MANAGEMENT GUIDELINES

Australian/New Zealand Standard for Risk Management

One resource that is available to assist NSW government agencies, such as NSW Police, with organisational risk management is the Australian/New Zealand Standard for Risk Management (*AS/NZS 4360:2004*), This standard describes itself as a 'generic guide for managing risk' that 'may be applied to a very wide range of activities' (Standards Australia & Standards New Zealand 2004a, p. 1). The Public Accounts Committee (2005) described the Australian/New Zealand Risk Management Standard favourably. In the report on its inquiry into risk management in the NSW public sector, the Public Accounts Committee found that:

> the majority of agencies surveyed either had well developed risk management practices or provided details of strategies being undertaken to move towards the best practice requirements of the *Australian/New Zealand Standard AS/NZS 4360:2004* (2005, p. vii).

The Public Accounts Committee report observed that the *AS/NZS 4360:2004* is 'seen as an effective tool in establishing sound risk management practices'. The Public Accounts Committee quoted Felix Klomen, whom it described as a leading US risk management expert, as stating that:

> AS/NZS 4360:2004 was and still remains the clearest and most concise guideline yet published (Public Accounts Committee 2005, p. 35).

From correspondence it has received, the Commission is aware that several Australian law enforcement agencies use *AS/NZS 4360:2004* as the basis for risk management within their organisations.

In the foreword to this Risk Management Standard, Standards Australia and Standards New Zealand describe risk management in the following way:

> Risk management involves establishing an appropriate infrastructure and culture and applying a logical and systematic method of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organizations to minimize losses and maximize gains.
>
> To be most effective, risk management should become part of an organization's culture. It should be embedded into the organization's philosophy, practices, and business processes rather than be viewed or practiced as a separate activity. When this is achieved, everyone in the organization becomes involved in the management of risk (2004a, p. v).

The *Australian/New Zealand Risk Management Standard AS/NZS 4360:2004* advocates a seven-step risk management process:

a. ***communicate and consult*** – with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.

b. ***establish the context*** – establish the external, internal and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined.

c. ***identify risks*** – identify where, when, why and how events could prevent, degrade, decay or enhance the achievements of the objectives.

d. ***analyse risks*** – identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk. This analysis should consider the range of potential consequences and how these could occur.

e. ***evaluate risks*** – compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.

f. ***treat risks*** – develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.

g. ***monitor and review*** – It is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvements. Risks and effectiveness of treatment measures need to be monitored to ensure changing circumstances do not alter priorities.

> For each stage of the process records should be kept to enable decisions to be understood as part of a process of continual improvement (Standards Australia & Standards New Zealand 2004a, pp. 7-8).

While the Standard, itself, provides information about how to undertake each step of the risk management process, further detailed guidance is provided in the Handbook that has been prepared to supplement the Standard (Standards Australia & Standards New Zealand 2004b).

Other risk management guidelines

The Public Accounts Committee also referred to the guidelines developed by the Treasury Managed Fund (TMF). The Public Accounts Committee reported that the TMF developed the *TMF Guide to Risk Management* to encourage a more consistent and improved approach to risk management, this guide is not mandatory and its use is not widespread (Public Accounts Committee 2005, p. ix). Despite the low usage rate, the Public Accounts Committee report observed that the inclusion of a reference list of other publications and resources that may assist agencies in developing their risk management practices is a useful feature of the TMF Guide (Public Accounts Committee 2005, p. 36).

When writing about risk management and policing in the United States, Archbold observed that there is not one best risk management process that is suggested to be used universally or for specific types of organisations (Archbold 2004, p. 40). However, she stated that there are five basic steps that are applicable to most types of organisations:

- identify risks, frequency of exposure to risks, and the severity of losses resulting from exposure to risks
- explore methods to handle exposure to identified risks
- choose appropriate treatment or response to manage exposure to risks
- implement risk treatment, and
- continuously evaluate risk treatment applied to organisational risks (Archbold 2005, p. 31).

Archbold stressed that the risk management process is not over after all five steps have been completed. She stated that the risk management process is continuous because organisational risks change over time and continuously require re-evaluation (Archbold 2004, p. 48).

While different authors divide the risk management process into slightly different steps, there is commonality in the nature of the steps and processes described (see, for example, Archbold 2004, pp. 39-48). All see the process as a continuing one, with an emphasis on communication, monitoring and review.

MISCONDUCT RISK MANAGEMENT GUIDELINES

Australian Fraud and Corruption Control Standard

Guidance that focuses specifically on misconduct risk management is also available. Standards Australia has produced an Australian *Fraud and Corruption Control Standard AS 8001-2003*. Standards Australia recommends that agencies periodically conduct a comprehensive assessment of fraud and corruption risks within their business operations (2003, pp. 14-15). This Fraud and Corruption Control Standard includes guidance for applying the Risk Management Standard (*AS/NZS 4360:2004*) to the assessment of fraud and corruption risk (pp. 21-25).

Resources produced by the Independent Commission Against Corruption

The Independent Commission Against Corruption (ICAC) has produced a number of resources to assist NSW public sector agencies to identify, assess and treat their corruption risks. For example, in the 'Corruption risk assessment and management module' of its 1996 *Practical Guide to Corruption Prevention*, the ICAC outlines a nine-step process:

i. identify the major functional areas of the organisation
ii. identify the risks for each functional area and assess the extent of these risks
iii. identify the significant risks and assess the probability of those risks occurring
iv. identify responses to risk areas
v. select the best response
vi. develop risk management measures
vii. formalise and document a Risk Management Plan
viii. implement the Risk Management Plan
ix. review and evaluate the Risk Management Plan and its implementation (ICAC 1996, pp. 4-8).

One of the topics covered in the ICAC's 2002 *Do-it-yourself corruption resistance guide* is 'Corruption Risk Management'. This guide describes five levels of achievement that an agency can reach in terms of its corruption risk management. The ICAC describes the lowest level of achievement as:

> Risk management is practised in isolated areas of the agency and/or on an ad hoc basis. Some staff are aware of the risks.

and the highest level of achievement as:

> The agency has a comprehensive risk plan that identifies risks, the measures taken to minimise the impact of these risks, assigns roles and responsibilities and provides for regular monitoring and review. Regular monitoring and review occurs (ICAC 2002, p. 16).

A third ICAC resource in this area was provided in 2003 when the ICAC published its profile of functions, corruption risks and corruption resistance strategies across the NSW public sector. The objectives of this research included, amongst others, identifying differences among public sector organisations in respect of the corruption risks they face and the prevention strategies they have in place, as well as promoting a broader discussion of the corruption risks facing the NSW public sector. Its report also demonstrated a four-part process that agencies can use to analyse their own corruption risks. This process involved:

- examining the nature of the work undertaken to consider 'high-risk functions'

- asking those who know the organisation best what they consider the corruption risks to be
- identifying the strategies in place to treat the misconduct risks that have been identified, and
- examining staff awareness of relevant policies and processes (ICAC 2003).

RESEARCH ON RISK MANAGEMENT IN LAW ENFORCEMENT

There is little available research on risk identification, assessment and treatment in law enforcement agencies in the United States. In her review of the literature on risk management in law enforcement agencies in the United States, Archbold (2004) observed that at that time there had only been one book and six magazine and journal articles written by professionals with experience working in risk management in law enforcement. She further observed that none of these had been based on data collection or analysis of data from police agencies (Archbold 2004, p. 157).

Having identified a lack of prior research on this topic, in 2001 Archbold conducted a telephone survey of all 354 United States municipal and county law enforcement agencies that employ 200 or more sworn officers. She found that only 14 of these 354 law enforcement agencies reported using risk management as one of their tools to control police related liability (Archbold 2005, pp. 30, 31).

Unlike their American counterparts, police departments in England and Wales compile annual threat assessments of their vulnerability to corruption. A recent report by Her Majesty's Inspectorate of the Constabulary (HMIC) found that 'while all forces reported having compiled threat assessments of their vulnerability to corruption, the standard and timeliness of submissions varied considerably' (HMIC 2006, p. 106). The National Crime and Intelligence Service (NCIS) collates the assessments made by the individual police departments to build a 'national picture'.

Given the reliance of any counter-terrorism policing on information management, of particular interest to the Commission's current assessment of the management of misconduct risks, was the NCIS's finding in its 2005 threat assessment that the 'most common and damaging type of corrupt action is the unauthorised disclosure of police information' (HMIC 2006, p. 106). The HMIC report further noted that:

> In May 2005, the annual conference of ACPO's [the Association of Chief Police Officers'] Professional Standards Committee (PSC) considered the national threat assessment in more detail and highlighted three primary areas of focus for the Service:
>
> - information leakage
> - infiltration of the Police Service, exacerbated by the ever-expanding 'extended police family'; and
> - substance misuse, with all its criminal conduct connotations and the additional risk of targeting, coercion or blackmail of staff (HMIC 2006, p. 106).

5.2 PROCESSES USED BY NSW POLICE AND THE CTCC

To gather information for this assessment, the Commission wrote to the Deputy Commissioner of Specialist Operations to obtain corporate-level information and to the Assistant Commissioner Counter Terrorism to obtain command-level information. In both requests the Commission sought copies of relevant documentation.

In relation to risk management processes at the corporate level, the Commission asked whether:

- NSW Police has a Service-wide policy or process it uses for identifying, documenting and managing risks, and if it does, whether this policy or process includes identifying and documenting organisational and/or command-level misconduct risks and misconduct prevention strategies
- there are any specific areas within NSW Police that have been assigned responsibility for oversighting misconduct risk management across the organisation as a whole or within the individual commands
- NSW Police has issued any statements or directions concerning command responsibilities for misconduct risk management
- NSW Police has provided any resources to assist commands in the process of identifying, assessing and managing misconduct risks
- NSW Police monitors the effectiveness of the treatment strategies used to reduce or manage individual misconduct risks.

In relation to risk management processes at the command level, the Commission asked:

- whether there is an individual, group or committee responsible for identifying, reducing and/or managing misconduct risks faced by officers working in the CTCC
- how misconduct risks are identified and assessed within the CTCC, and more specifically
    - what processes and sources of information are used for identifying misconduct risks
    - whether some assessment is made of the relative seriousness of the different misconduct risks, and if so, how that assessment is made
    - how the Command determines the best way of responding to each of the identified misconduct risks
    - to whom the identified misconduct risks and management strategies are reported
    - what resources are available to implement the risk management strategies

- whether the risk management processes used by the CTCC are different from the processes used to identify, assess and manage misconduct risks within NSW Police generally
- what, if any, help or resources are available to assist the CTCC identify and manage misconduct risks within the Command
- whether it is intended that the misconduct risks faced by officers working in the CTCC or the risk reduction or management strategies be reviewed from time to time and if so, what would trigger such a review, and
- whether the CTCC monitors the effectiveness of the treatment strategies used to reduce or manage individual misconduct risks.

The corporate-level answers[4] and the command-level answers[5] to these questions are outlined in the following sections.

NSW POLICE – CORPORATE STRATEGIES

Command Management Framework

NSW Police informed the Commission that its 'Command Management Framework' (CMF) is the tool it uses for identifying, documenting and managing risks. NSW Police also advised that corruption resistance is a major component of one module of this tool ('people management'). It described the CMF as 'the core tool for the risk management of corporate objectives, customer service and employee behaviour' and 'a move away from compliance based auditing to a risk based self-assessment audit process which has been identified as best practice'.

The material concerning the CMF, supplied by NSW Police from its intranet, states that commands need to tailor the CMF to their own requirements and that responsibility for administering the CMF rests at the command level:

> We acknowledge that one size does not fit all and we therefore encourage local commands to adapt the CMF to their own needs.
>
> For Risk Management to be effective, individual commands need ownership of the internal control process. Accordingly the Service is moving from Compliance Based Auditing to a Risk Based Self-Assessment Audit Process (the CMF).
>
> Self assessment … [provides] a balance between reporting needs and unnecessary external scrutiny. It systemised the checking function, identified as a Service shortcoming during the Wood Royal Commission. …

[4] Throughout this and subsequent chapters, the corporate-level responses are taken from a letter from NSW Police Deputy Commissioner Specialist Operations to Commissioner Police Integrity Commission dated 12 April 2006, received 26 April 2006.

[5] Throughout this and subsequent chapters, the command-level responses are taken from a letter from NSW Police Deputy Commissioner Specialist Operations to Commissioner Police Integrity Commission dated 20 April 2006, received 20 April 2006.

> Command management, utilising the CMF, will now have responsibility for conducting regular risk driven self-assessments. This reduces the need for external audits. Commands will have more responsibility for monitoring their own performance against the key priorities:
>
> - crime reduction
> - rationalised and improved work practices
> - employee job satisfaction and motivation
> - public satisfaction and police responsiveness (NSW Police intranet, downloaded by NSW Police 30 March 2006, provided to the Commission 26 April 2006).

The CMF is divided into the following modules: People, Crime; and Systems. The material from the NSW Police intranet states that corruption resistance (or strategies to minimise misconduct) forms one part of the People Management Module of the CMF:

> … Corruption resistance is a major component of the People Management Module of the CMF. This module provides an effective tool to continually improve the management of corruption resistance activities and complaints handling procedures (NSW Police intranet, downloaded by NSW Police 30 March 2006, provided to the Commission 26 April 2006).

In relation to implementing the CMF, the material supplied by NSW Police from its intranet lists the following 'suggested implementation approach':

> - Consult with staff
> - Identify risk/priority areas
> - Establish teams
> - Allocate portfolio holders and back up officers
> - Set time frames – monthly reporting or similar
> - Conduct quarterly reviews of portfolios and teams to evaluate/monitor performance
> - Conduct test sampling/quality review e.g. DO, LAM, CM, SOM's
> - Link CMF to performance agreements/command assignments
> - Link CMF to business plans
> - Identify issues for continuous improvement (NSW Police intranet, downloaded by NSW Police 30 March 2006, provided to the Commission 26 April 2006).

No further elaboration was provided on any of the steps of this suggested implementation approach.

The information provided about the NSW Police CMF specifically discussed the links between the CMF and each of the Australian Business Excellence Framework, Appendix 31 of the report of the Royal Commission (which described details of the proposed external audit of the reform process) and the NSW Police Service Future

Directions statement. However, it did not explicitly make any reference to any links between the CMF and the Australian/New Zealand Risk Management Standard *AS/NZS 4360:2004*.

Assessment of risks

The material supplied by NSW Police from its intranet describes risk assessment as requiring an estimate of the likelihood and the consequences of an event:

> Risk is the chance of something occurring and its impact on our corporate objective. In order to manage risk, an estimate of the likelihood and consequences must be made. When these two factors are combined, a decision can be on the level of risk. All events or risks need to be monitored. A change in the likelihood or the consequence is likely to have an effect on the assessment of the risk.
>
> Risk/priority assessment involves three stages:
>
> - assessing likelihood
> - assessing consequence
> - risk/priority rating (likelihood x consequence = risk) (NSW Police intranet, downloaded by NSW Police 30 March 2006, provided to the Commission 26 April 2006).

Other resources provided to commands

When asked whether it has provided any resources to assist commands in the process of identifying, assessing and managing misconduct risks, NSW Police responded that it has 'a wide range of instruments and procedures which specifically encompass the task of assessing and managing behaviour and/or misconduct risks'. It provided a list of 'risk identification, assessment and management instruments and procedures' within NSW Police. In this list, NSW Police did not distinguish between resources that apply to risk management and the resources that apply to the management of individuals who have been found to have engaged in misconduct in the past. The Commission has grouped this list of resources into the following categories:

- resources that document guidance on acceptable behaviour and NSW Police values (specifically the Code of Conduct and Ethics, the Statement of Values, the Oath of Office, and the Code of Conduct for Students)
- legislation (specifically the *Police Act 1990* (section 181D and 173), Police Regulation 2000, *ICAC Act 1988*, *Public Sector Employment and Management Act 2002*, *Protected Disclosures Act 1994*, Integrity Testing Legislation)
- components of the NSW Police complaint management system and management action process (C@ts.i, Commissioner's Advisory Panel, Internal Review Panel, Complaint Management Teams, Local Management Issues).

Other types of resources that were listed were not as easily grouped, for example: 'Professional Standards Command', 'Police Employee Corruption Hotline', and 'Customer Assistance Unit (PAL)'.

Subsequently NSW Police advised the Commission that its intranet contains a link to the Australian/New Zealand Risk Management Standard to enable this Standard to be accessed by its officers and that training provided in the Sergeants' Course includes a reference to this Standard.

NSW Police also advised that the Professional Standards Command offers consultancy regarding complaints through its Complaints Management Support Unit and analytical products through its Intelligence Unit's Strategic Research Team. The two analytical products that were specified were Officer Complaint Analysis (OCA) and Environmental Scans:

> Officer Complaint Analysis (OCA): The OCA assists commanders when developing timely intervention strategies designed to minimise the risk of officers receiving further complaints. The intention is to identify trends for early intervention. An OCA can be requested on an officer who is considered at risk of attracting complaints by their Commander or Professional Standards Manager.
>
> Environmental Scan: The aim is to provide an understanding of the nature of complaints received at a command and the demographics of officers at risk. The analysis informs commanders in developing timely intervention strategies with a view to minimising the risk of officers receiving further complaints.

When the Commission sought additional information on OCAs and Environmental Scans, it learnt that the first OCA was completed in NSW Police in November 2002 and that no request had been made for an OCA for any officer attached to the PSG, CTCC or PORS. The first Environmental Scan was completed in NSW Police in March 2003 and no Environmental Scan has been prepared for the CTCC or PORS.

Monitoring and review of effectiveness of the risk management process

When asked whether it monitors the effectiveness of the treatment strategies used to reduce or manage individual misconduct risks, NSW Police responded in terms of how it monitors the progress of individual officers who have engaged in misconduct rather than how it has monitored the treatment of the misconduct risks:

> Employee Management within the Human Resources Command conducts a positive and proactive process in regard to the established or possible misconduct of individuals through Remedial Performance Programs, Procedures and Plans. Such practices are closely related to the CMF.

CTCC – COMMAND-LEVEL STRATEGIES

The CTCC said that the processes that it uses to identify, assess and manage misconduct risks are not different from the processes used within NSW Police generally.

Responsibility for misconduct risk management

When asked whether there is any individual, group or committee responsible for identifying, reducing and/or managing misconduct risks faced by officers working in the CTCC, the CTCC responded:

- Individuals within the Command are aware of their obligation in relation to the NSW Police Code of Conduct and Statement of Values, Commissioner's Statement of Professional Conduct
- Management meetings are conducted monthly providing a forum for issues to be raised and addressed. These issues include risk issues and may include misconduct issues
- Complaints Management Team assesses and manages using the [NSW Police] Complaints risk management model
- HR Committee provides recommendations to the Commander re the recruitment and management of staff
- Operation Review Committee (comprising the Commander, Unit leaders and other staff – meeting three times a week) monitor, discuss and review information and intelligence taskings
- NSW Police Command Management Framework operates within the Command with each Unit monitoring the results and oversighted by the Commander. This Framework is based on risk assessment and the level of monitoring is commensurate with the identified level of risk. Regular reporting of these issues provides the opportunity of reviewing the level of risk and adjusting monitoring to cater [for] increased or indeed decreased levels of risk.

Process for identifying misconduct risks

In its response to the Commission, the CTCC listed the following processes and sources of information as ones that it uses to identify misconduct risks:

- Command Management Framework
- Complaint Management Team
- Ensure compliance with Secondary Employment Policy
- Gift register
- Assets management
- COPS audits

- Monitor access control
- Monitor systems in use (ie internet)
- Safe storage and handling of documents/information (per Australian Government Protective Security Manual and corporate policies and procedures)
- Integrity checking when coming to Command
- Commander liaison with Stakeholders
- Telephone usage audits
- Operational Review Committee processes
- Performance Management Scheme (PMS).

When asked, the CTCC identified a number of factors that could trigger the Command to review the misconduct risks faced by its officers. It said that these factors include: the 'time period since the last review', 'issues that are identified', 'changes to existing work environment or exposure to a new environment', 'set time periods', 'CMF results', 'audit results', 'trends identified in the complaints', and/or the 'introduction of new legislation, policies or procedures'.

Process for assessing misconduct risks

The CTCC told the Commission that it makes an assessment of the relative seriousness of different misconduct risks proactively through the Command Management Framework and reactively through the Complaints Management Team (CMT). In its response, the CTCC explained that the CMF 'rates risks of differing systems and processes throughout the Command'. It further elaborated that 'this framework allows checking against compliance and reassessment of risk if misconduct or procedural shortcomings are identified'. The CTCC's response also referred to a 'post-event review and analysis of complaints by the CMT allows for causal factors to be identified and treatment options applied' such as amending the CMF to cater for the newly identified risks. Furthermore it said that as part of its review of complaints 'the CMT is in a position to rate the seriousness which is usually conducted using corporately determined criteria'.

When describing its process for assessing the seriousness of misconduct risks, the CTCC did not explicitly refer to considering the likelihood or the consequences of the risks.

Process for identifying appropriate treatment of misconduct risks

The CTCC said that it determines the best way of responding to each of the misconduct risks through:

- Discussions at the Command Management meetings and Complaint Management Team meetings
- Consultation with specialists such as Professional Standards Command (PSC)
- Development of policies (SOPs) and guidelines established
- Preparation and presentation of induction packages

- Participation in Performance Management Scheme and other Employment Management policies
- Amendment of the Command Management Framework.

Documentation

When asked for documentation that might demonstrate its risk management processes, the CTCC provided the Commission with a copy of its CMF framework and documentation of its Induction Package.

The CTCC Command Management Framework

In the documentation of its Induction Program the CTCC describes its CMF as follows:

> The Counter Terrorist Command has established a Command Management Framework in line with Legislative requirements.[6] The CMF assists the Commander to manage operations and improve accountability at all levels. The CMF is a self-audit tool for the Command along with monitoring our own performance against the key priorities, which are:
>
> - Rationalised and improved work practices
> - Employee job satisfaction and motivation
> - Public satisfaction and police responsiveness.
>
> Officers within the Command have been assigned 'Portfolio's' and have delegated tasks to attend to on a regular basis. Sampling of the process is scheduled periodically in order to satisfy the reviewing officer that the portfolios are being managed efficiently (CTCC Induction Program, p. 18).

The CMF consists of a series of Excel spreadsheets or 'templates'. As stated above, the different aspects of the CMF (or portfolios) have been assigned to different areas within the CTCC:

- the Investigations Unit makes checks concerning Accountable Operational Books, Arms and Appointments, Brief Management, DNA Exhibits, Case Management, COPS[7] Management, Drug Bag Allocation Register, e@gle.i Management, Fleet Management, Investigation Case Files Management, Mobile Telephones, Portable Equipment, and Search Warrants
- the Intelligence Unit makes checks concerning Accountable Operational Books, Arms and Appointments, ASAP, ASNET/Speakeasy, Case Management, COPS Management, Fleet Maintenance, Intelligence Management, Internet, Mobile Telephones, Pigeon Holes, Portable Equipment, and TRIM Management

[6] It is not clear which 'Legislative requirements' are referred to here.

[7] Computerised Operational Policing System (NSW Police data system)

- the Dignitary Protection Unit makes checks concerning Arms and Appointments, Consulate Liaison, Fleet Maintenance, Malicious Call Traces, Occupational Health & Safety, Pigeon Holes, Portable Equipment, Safe Driver Policy and Security Reviews.

The CTCC provided the Commission with copies of the templates for each of these 'portfolios'. The nature of the material included in these templates is diverse:

- on some occasions the entries appear to refer to responsibilities for specific positions, for example: one entry on the 'Intranet' template states: 'Ensure that the CTCC site is regularly updated and that the information stored on the site is current'
- on some other occasions the entries in the CMF appear to refer to activity counts, for example, on the 'Consulate Liaison' template, one entry states: 'Number of consular functions attended, consular security coordinated'
- in some templates the entries refer to having systems in place, for example: the template pertaining to Accountable Operation Books requires the supervisor 'to have a checklist system in place to ensure that accountable operational books are inspected for quality and compliance – duty books (weekly) and notebooks (fortnightly)'
- in some templates the entries in the CMF refer to risk treatment strategies, for example on the Fleet Maintenance Template one of the entries includes 'Vehicle diaries to be checked weekly to ensure compliance with [NSW Police] policy and procedures re use of vehicles'. Similarly, in relation to the Mobile Telephones template, it states that 'the Mobile Telephone Register is checked and endorsed monthly by the Supervisor to ensure that all items including handsets and sim cards are accounted for'.

Corruption resistance and the CTCC CMF

The CTCC Induction Program documentation describes that corruption resistance (or strategies to minimise misconduct) is a major component of one module of the CMF:

> Corruption resistance is a major component of the People Management module of the CMF. It provides an effective tool to continually improve the management of corruption resistance activities and complaints handling (CTCC Induction Program, p. 18).

However, when the Commission sought to obtain a copy of that section of the CTCC's CMF that deals with corruption resistance, the Commission was informed that there is no discrete section that relates to corruption resistance. Instead, the Commission was told that corruption resistance was built in overall within the CTCC's CMF.

Examination of CTCC Complaint Management Team meeting minutes

In addition to the CMF, the CTCC also identified the Complaints Management Team (CMT) as playing an important role in its misconduct risk management process. The CTCC referred to the CMT as one of the committees responsible for identifying risks

faced by CTCC officers as well as being responsible for assessing and monitoring these risks.

The Commission requested copies of the minutes of the CTCC's CMT meetings to better understand the role of this CMT in relation to misconduct risk management. The CTCC supplied the minutes for twelve meetings held between October 2004 and April 2006.

The Commission found these minutes to be clearly presented. These minutes documented:

- the status of investigations of complaints made against officers
- any new complaints received
- the progress of individual officers who were operating under a conduct management plan
- discussions of the results of COPS and RTA audits
- consideration of failed prosecutions, and
- general issues raised such as correspondence received from Professional Standards Command.

Information on the NSW Police intranet in relation to the 'management of actions & outcomes' states that:

> To enable CMTs to identify systems issues, recurring themes, emerging patterns in officer complaint histories and complaint turnaround times, they should maintain 'Complaint Trends' as a standing agenda item.

In the minutes of the CTCC's CMT meetings there was no mention of 'Complaint Trends' per se and hence no indication that it was a standing agenda item. However, within the CTCC's CMT meeting minutes there were clear examples of where the CMT had looked at the wider implications of individual complaints and where it had taken steps to tackle the issues underlying some of these complaints:

- in some cases the complaints led to all officers being sent reminders of specific policies: in one case an email was sent to all officers reminding them of their responsibilities in relation to the NSW Police Email Policy; in another case a direction was given to remind all officers to obtain approval from their supervisor prior to changing their shifts
- in relation to one set of COPS[8] and RTA[9] audits that were conducted, the CMT had noted a failure by some officers to supply their note book or duty book references to support their accesses to the information. It was further noted that the supervisors of those officers had failed to identify this deficiency. This led to the Commander deciding to speak with Unit Leaders to reinforce the correct auditing procedures

[8] Computerised Operational Policing System (NSW Police data system)

[9] Roads and Traffic Authority.

- following one complaint an officer was asked to prepare an information package for distribution within the command concerning legislation with which he had previously said he had not been familiar
- following another specific complaint, the CMT determined to conduct a comprehensive audit of a particular area of operation, review the current Standard Operating Procedures for that area and to implement a new recording system.

5.3 OBSERVATIONS

Although widely accepted, there is no requirement for individual agencies to comply with the Australian/New Zealand Standard for Risk Management (*AS/NZS 4360:2004*). What this standard provides is an indication of the types of steps that one would expect an organisation to follow as part of its risk management process. It specifies a continuing process which involves communication and consultation, establishing the context and criteria against which risks will be evaluated, identifying the risks, analysing the risks, evaluating the risks, treating the risks, and monitoring and review of the risks and the effectiveness of the treatment process. The standard also emphasises that records should be kept for each stage of the process to enable decisions to be understood as part of the process of continued improvement.

THE CORPORATE APPROACH

NSW Police has advised that the Command Management Framework (or CMF) is the tool that it uses for identifying, documenting and managing risks. The CMF takes the form of a series of Excel spreadsheets or 'templates'.

The Commission understands that the only requirements NSW Police places on commands in relation to the CMF are that individual commands should tailor the CMF to their own requirements and that they should take responsibility for administering the CMF.

It would appear that the effectiveness of the CMF as a risk management tool depends on how well it is tailored to address the risks faced by the individual command. Much of what the *AS/NZS 4360:2004* would describe as five of its seven-step risk management process – that is, communication and consultation, establishing the context, risk identification, risk analysis and risk evaluation components – would need to occur as part of the process to tailor the CMF to the specific risks facing the individual command. That is, while these steps of the risk management process may occur 'behind the scenes' in the development of a command's CMF, any strategies used are not visible from an examination of the resultant CMF. While NSW Police provides a 'suggested implementation approach' for the CMF on its intranet site, this does not provide any guidance on how commands should go about identifying, analysing or evaluating their risks or what level of documentation of the process is required. However, the Commission understands that internal advice is available to commands on these issues.

THE COMMAND-LEVEL APPROACH

The CTCC has advised that its approach to misconduct risk management does not differ from the corporate approach, that it to say, it uses the CMF. The CTCC has followed NSW Police requirements to tailor its CMF to its own requirements (for example by including a template on Consulate Liaison) and has taken responsibility for administering this tailored CMF. However, the nature of the material in the CTCC's CMF templates is diverse and it is unclear how these templates relate to the misconduct or other risks that may be facing the CTCC.

The CTCC, in its command-level response, has advised that it has a number of committees that are responsible for identifying, reducing and/or managing misconduct risks. It has listed fourteen different processes that it uses to identify misconduct risks as well as a number of factors which could trigger the command to review the misconduct risks faced by its officers.

The absence of documentation of the CTCC's risk management strategies means that it is difficult to assess how cohesive or comprehensive its current processes are. It is also not possible to determine how well the CTCC has tailored its CMF to meet its needs. Overall, the picture the CTCC provides of its risk management strategies is one incorporating a number of discrete elements where any interrelationships between the elements are not specified.

It is perhaps surprising that while lauding the value of a corruption resistance module in the CMF, the Commission was informed that there is no discrete section in the CTCC's CMF that relates to corruption resistance. Instead, the Commission was told that corruption resistance was built in overall within the CTCC's CMF.

5.4 SUMMARY OF KEY POINTS

1. The Australian/New Zealand Standard (*AS/NZS 4360:2004*) provides an accepted framework for how one might expect an organisation to undertake risk management.
2 The Command Management Framework (CMF), which provides templates for a 'risk based self-assessment audit', is the core tool that NSW Police advises that it uses for identifying, documenting and managing risks. Commands are responsible for tailoring the CMF to their own requirements and are responsible for administering the CMF within their command.
3. The CTCC uses the same risk management process (the CMF) as is used by other areas of NSW Police. Each unit of the CTCC is responsible for monitoring specific aspects of the CMF. While the CTCC has tailored its CMF to the needs of the command, it is unclear how well the templates of the CTCC's CMF reflect the command's specific misconduct or other risks.
4. Contrary to the corporate design, the CTCC's CMF does not contain a specific component that focuses on corruption resistance (that is, a component that focuses on strategies to minimise police misconduct). Instead the CTCC says that corruption resistance is built in overall within its CMF.
5. The CTCC describes its misconduct risk management strategies as a collection of discrete elements. The relationships between these elements are not specified.
6. The minutes of the CTCC's CMT meetings contain examples of where the CMT has looked at the wider implications of individual complaints and taken steps to tackle the underlying issues.
7. The effectiveness of the CMF as a command risk management tool depends on the effectiveness of the process used to tailor the CMF to the needs of the individual command – that is, the effectiveness of the process to identify, analyse and evaluate command risks. This process is not documented for the CTCC.

6. COUNTER TERRORIST COORDINATION COMMAND: FUNCTIONS AND ASSOCIATED MISCONDUCT RISKS

This chapter identifies the nature of the misconduct risks that are associated with the work of the CTCC. It commences with a description of the role, functions and structure of the CTCC. The chapter then examines the types of misconduct risks that might reasonably be expected to exist within any unit that performs the kinds of functions carried out by the CTCC. A description of the strategies that the CTCC uses to treat or respond to its misconduct risks is provided in Chapter 7.

6.1 ROLE, FUNCTIONS AND STRUCTURE

BACKGROUND

The CTCC is one of several units that report to the Deputy Commissioner Specialist Operations through the Assistant Commissioner Counter Terrorism and Public Order Management. According to the most recent organisational chart provided to the Commission (dated 23 February 2006), in addition to the CTCC, the State Protection Group (SPG), the Public Order and Riot Squad (PORS), the Counter Terrorism Response Coordinator, the Counter Terrorism Executive Advisor and the Critical Infrastructure Unit report to the Assistant Commissioner Counter Terrorism and Pubic Order Management.

MISSION AND ROLE

The following statement of the CTCC's mission is provided on the NSW Police website:

> To provide a comprehensive and co-ordinated response to acts of terrorism or politically motivated violence through intelligence collection, analysis, investigation services and protection operations for dignitaries, national icons, business interests and critical infrastructure.

The NSW Police website also lists the following as the principal roles of the CTCC:

- provide close personal protection for internationally protected persons, dignitaries and other persons as determined appropriate by the Commander, CTCC
- provide tactical intelligence gathering, analysis and investigation in relation to politically motivated violence, terrorist activity, public order, dignitary protection, critical infrastructure, consequence management, national icons, threats to high office holders, threats to the diplomatic and consular corp
- co-ordinate the NSW Police responses to politically motivated violence and terrorism in accordance with the National Counter Terrorist Plan and the NSW Police Counter Terrorist Plan

- liaise with, and provide advice to, clients with regard to the protection of critical infrastructure and consequence management, and

- provide strategic analysis, advice and direction to clients in relation to the security environment of NSW.

CHARTER

As was the case for the PSG, the activities of the CTCC are governed by a charter which outlines the CTCC's functions and elements of its management structure. This charter specifies that the CTCC has a number of functions, including:

> a. to oversight the provision of dignitary protection work
>
> b. to coordinate the police response to terrorist acts
>
> c. (i) to coordinate police investigations following a terrorist act
>
> (ii) to coordinate police investigations of any persons suspected of intending or conspiring to effect a terrorist act
>
> (iii) to take command of such investigations where directed by the Commissioner of Police
>
> d. to gather intelligence and conduct investigations of suspected terrorists and terrorist acts, with a view to prevention of terrorist incidents through disruption, apprehension, criminal prosecution and incarceration
>
> e. to represent police, or provide support for the police representative in relation to the National Counter Terrorism Plan, the NSW Emergency Management Plan and other law enforcement and national security agencies in relation to counter terrorism issues
>
> f. to provide advice to stakeholders, including custodians of critical infrastructure, in relation to terrorism issues, and in relation to security measures (NSW Police Counter Terrorist Co-ordination Command Charter 2003, p. 1).

The Charter of the CTCC specifies limits to the range of intelligence activities and investigations it should undertake:

> The CTCC is to ensure that intelligence and investigatory operations are limited to persons who are reasonably suspected of terrorist acts, and the CTCC shall not conduct investigations of persons solely on the basis of political views, except to the extent that the expression of those views may constitute crimes (NSW Police Counter Terrorist Co-ordination Command Charter 2003, p. 1).

The Charter also provides guidance as to how records should be kept:

> The CTCC will keep proper records of all its operations. In particular, records of intelligence and investigations operations must be in a form consistent with the audit obligations under part 3 of the Police Act [to be

> amended][10], e@gle.i is to be the investigations management system used by all members of the CTCC (NSW Police Counter Terrorist Co-ordination Command Charter 2003, p. 3).

According to its charter, the management structure of the CTCC must include a Counter Terrorism Management Committee (CTMC) comprised of the Commissioner of the NSW Crime Commission (as chair), the NSW Police Deputy Commissioner responsible for the CTCC, and the Director-General of the Ministry for Police. The CTMC is responsible for overseeing the discharge of a number of the CTCC's functions relating to counter-terrorism, together with any participation in any joint operational arrangement with other agencies such as the Australian Security Intelligence Organisation (ASIO), and the Australian Federal Police (the AFP). The charter clarifies that 'the CTMC will not exercise command nor control over CTCC personnel' (NSW Police Counter Terrorist Co-ordination Command Charter 2003, p. 2).

In relation to the CTMC, in its corporate-level response NSW Police stated:

> The management committee will not be involved in the day to day administration and control of CTCC personnel. This function will be akin to existing procedures for all commands within [NSW Police], that is, the CMF.

STRUCTURE OF THE CTCC

The CTCC is composed of three different work units:

- **Dignitary Protection Unit** is responsible for providing close personal protection to 'at risk' dignitaries (both foreign and domestic). Among other functions, it also coordinates and plans security escorts, and provides specialist advice to Regions and Local Area Commands in the planning and co-ordination of a policing response to dignitary protection, major event and public order management issues involving terrorism or politically motivated violence. It liaises with national and international agencies involved in the protection of 'at risk' dignitaries, and it conducts physical security reviews and assessments.
- **Intelligence Unit** provides NSW Police with a specialised strategic, operational and tactical intelligence service in relation to politically motivated violence including extremist activity and acts of terrorism. This includes the preparation of risk and threat assessments, National Security Hotline disseminations, National Security Threat Assessments, dignitary protection intelligence support, investigations intelligence support, field intelligence support, aviation and maritime liaison, counter intelligence. This unit provides professional oversight of the intelligence support for the SPG and for the PORS. It also manages the CTCC information management systems and COPS intelligence components for the CTCC, as well as internal and external agency liaison.

[10] No explanation is provided in the charter as to the nature of the amendment to Part 3 of the Police Act referred to here.

- **Investigations Unit** is responsible for investigating offences relating to the threat of politically motivated violence including threats of terrorism, or threats against high office holders. In the case of a major terrorist incident, this unit may conduct a joint investigation with other NSW Police groups (such as the State Crime Command, Forensic Service Group, Special Services Group and relevant Local Area Command) or relevant external agencies (particularly the AFP and ASIO). It is also responsible for investigating credible threats of terrorism (for example, alleged terrorist training camps, suspect financial activity or in response to information provided by other agencies). Critical to this role are the following activities:
    - conducting proactive investigations regarding suspected targets
    - liaison with other agencies and sharing information on investigations, and
    - use of covert evidence gathering techniques.

The unit leaders of each of these units report to the Commander of the CTCC.

FEATURES OF THE CTCC'S WORK

The Commission considers that several features of the CTCC's work are noteworthy:

1. it is **broader than counter-terrorism policing**
2. it is **specialised**
3. much of the work is **covert,** hence it is not open to public scrutiny
4. the work **can become high-profile** (particularly if something goes wrong, as was the case in England when on the 22 July 2005 officers from the Metropolitan Police Service 'shot dead an innocent man' (Blair 2005, p. 2))
5. **the work of the CTCC encompasses many of the same functions that were undertaken by its predecessors, the Special Branch and the PSG** – it involves the protection of dignitaries as well as analysis, information gathering and liaison in relation to politically motivated violence including terrorist activity – hence it would be incorrect to base an argument that the risks and oversight arrangements required of the CTCC are different from those of the former Special Branch or the former PSG on the premise that the functions of the CTCC are different from those of its predecessors
6. it has the **same combination of functions that caused the Privacy Committee to recommend that the former Special Branch 'should have a more limited entitlement to collect intelligence than would normally be given to a Police force**' (Privacy Committee 1978, p. 26). When describing the functions of the former Special Branch, the Privacy Committee wrote:

> … the Committee considers that the Branch should be mindful of its different functions, wherever possible. The wider powers particularly those of enforcement, held by the Special Branch, as an arm of the NSW

> Police Force, carry with them responsibilities which may not apply as clearly to purely executive intelligence organisation (sic) (Privacy Committee 1978, p. 22).

More recently, when discussing covert search warrants, the Australian Muslim Civil Rights Advocacy Network (AMCRAN) wrote:

> At the core of the problem is that NSW Police in executing such warrants are behaving in an intelligence-gathering capacity rather than a law enforcement capacity. These two capacities are important to separate – and that is why the functions and duties of ASIO and the Australian Federal Police are distinguished (AMCRAN 2005).

7. the work has a **preventative focus** with the consequence that much of the information collected by the CTCC is gathered in an attempt to prevent future threats of terrorism or other forms of politically-motivated violence or attacks on dignitaries which have yet to occur. This preventative focus distinguishes its information collection from that in many other areas of policing
8. the nature of the work may cause some people to **fear the creation of 'dirt files', even if this fear is misplaced**. Hocking (2003) cited Justice Lionel Murphy's minority judgment in the *Church of Scientology* case in 1982 in which Justice Murphy described the consequences of intelligence collection including the generation of a climate of apprehension. Hocking stated that Justice Murphy:

   > reflected on the need for adequate legislative control and oversight of security organisations, recognising in particular that the practice of political surveillance in the civic arena and the public awareness of this practice, generates what he termed; 'a climate of apprehension and an inhibition of lawful political activity even at the high levels of government … Experience thus shows [Murphy continued] that for a free society to exist intelligence organisations must be subject to administrative supervision and amenable to legal process' (Hocking 2003, p. 7).

9. **some of the information collected is likely to be irrelevant and some assessments are likely to be subjective**: When discussing the nature of the information collected by the former Special Branch, the Privacy Committee wrote:

   > … we believe the Police will invariably accumulate a certain amount of possibly irrelevant and subjective data about the subjects of their files. The high degree of risk involved in this collection practice which we believe can be justified in the interest of Branch efficiency must be countered by strict security measures (Privacy Committee 1978, p. 26).

10. in most cases the **information collected will be incomplete**
11. the work requires strong **cooperative, coordinated and consultative relationships with officers from a range of federal and state agencies** (National Counter-Terrorism Committee 2005, p. 1.2), including work as part of Joint Counter-Terrorism Teams (National Counter-Terrorism Committee 2005, p. 4.4), and frequent liaison with the Australian Federal Police, Australian Security Intelligence Organisation, Protective Security Coordination Centre, Department of Foreign Affairs and Trade and the NSW Consular Corps (CTCC Induction Program (undated), p. 7).

In addition, it is also noteworthy that the structure of the CTCC has been **subject to continuing change.** During the period that the Commission was collecting information for this assessment (late 2005 to mid-2006) a number of changes occurred or were foreshadowed to occur, including:

- the creation of the Public Order and Riot Squad (PORS) and its location within the renamed Counter-Terrorism and Public Order Management Group
- the relocation of the Vikings Unit within the Counter-Terrorism and Public Order Management Group
- a new Assistant Commissioner Counter Terrorism and Public Order Management commenced duties on 3 April 2006
- at the end of June 2006, an in-principle agreement to co-locate the investigation team, together with their intelligence support with the NSW Crime Commission and AFP investigators, and the establish a joint management arrangement governed by a new Tri-Partite MOU were foreshadowed. At that stage it was known that further consultation would be required regarding data management arrangements, among other things.

6.2 MISCONDUCT RISKS POTENTIALLY FACED BY OFFICERS WORKING IN THE CTCC

The Commission used a variety of methods to identify the misconduct risks that might reasonably be expected to be faced by officers working in the CTCC as a function of the nature of the work they carry out. The approach involved both asking NSW Police (at the corporate level, at the command level and at the CTCC supervisor level) what they consider to be the main misconduct risks, as well as identifying misconduct risks from a range of other sources (such as the literature on police misconduct and previous inquiries disclosing problems in areas with similar functions, complaints made about officers working in the CTCC, consultation with law enforcement agencies from other jurisdictions that carry out similar functions) to attempt to identify any additional misconduct risks that may have been inadvertently overlooked by NSW Police.

From the responses received it is clear that there was no consolidated list of the misconduct risks that may face those working in the CTCC.

A summary of the potential misconduct risk areas identified from these different sources is provided later in this chapter in Table 6.1.

POTENTIAL MISCONDUCT RISKS IDENTIFIED BY NSW POLICE

One recognised strategy for identifying corruption risk areas is to ask those who know the organisation best what they consider the corruption risks to be. Perceived risks are important because if organisations do not identify something as a misconduct risk they will be less likely to attempt to manage that risk (Gorta 2002, Gorta 2006, p. 211). As the ICAC has noted, when organisations report what they see as their corruption (or misconduct) risks they are identifying activities that they believe could occur and, if they did occur, would have a negative impact on the work

of the organisation. They are not necessarily referring to events that have occurred (ICAC 2003, p. 5). Furthermore, when considering these perceived misconduct risks, it should be remembered that not all risks are equal. Some misconduct risks are more likely to occur than others and some would have a greater impact if they were to occur.

Potential misconduct risks identified in written NSW Police corporate-level response

When asked whether the CTCC is recognised by NSW Police as a command for which special misconduct risks exist due to its functions, NSW Police responded that it was unaware of any identified specific misconduct risks derived from the CTCC's functions. It added that 'individual commands including the CTCC, are encouraged by the CMF process to develop local input and processes relevant to their environment'.

When asked whether the misconduct risks specifically facing officers working in the CTCC have been identified and documented, in its corporate-level response NSW Police said that it:

> Is unaware of any misconduct risks specifically facing officers working in the CTCC being identified and documented.

Potential misconduct risks identified in written CTCC command-level response

In its response to the Commission, the CTCC said that there is no consolidated documentation of the misconduct risks identified as being faced by officers working in the CTCC. However, when asked 'what misconduct risks have been identified as potentially being faced by officers working in the CTCC as a result of the types of work carried out by the CTCC', the command identified the following list of potential misconduct risks:

- Unauthorised release or misuse of information – either deliberately or accidentally – especially information provided from third parties
- Inappropriate storage of information
- Inappropriate collection of information
- Recruitment of officers for information by external agencies (national security issue)
- Improper associations
- Misuse of motor vehicles
- Misuse of mobile phones
- False overtime claims
- Misuse of covert licenses.

The first four of these were considered to be 'moderate' risks by the Command, while the last five were considered to be 'minor' misconduct risks. The CTCC did not elaborate further on these potential misconduct risks.

Additional risks identified in structured interviews with senior staff

In the structured interviews that Commission officers conducted with key CTCC and PORS officers, officers were asked what they considered to be the major misconduct risks faced by officers working in the CTCC. As can be seen from Table 6.1, in their responses, these officers mentioned each of the risks listed above other than the last two: 'false overtime claims' and 'misuse of covert licences'. In addition, the officers interviewed also identified the following misconduct risks:

- Compromise of, or impropriety in, investigation
- Informant management
- Officers acting outside their charter
- Covert search warrants
- Security of exhibits/Exhibit handling
- Drug and alcohol abuse[11].

In relation to staff working in PORS, the risk of 'inappropriate use of force' received a special mention.

Some of those interviewed were not sure whether the misconduct risks were documented or not. One said that he thought that the generic risks would be in the Code of Conduct and Ethics. Another said that he thought that the CMF documents a range of risks including misconduct risks. Another officer said that some of the misconduct risks would be documented in the CTCC's Standard Operating Procedures (SOPs) and in its CMF, though he added that he had not seen a consolidated list.

POTENTIAL MISCONDUCT RISKS IDENTIFIED THROUGH OTHER SOURCES

From the literature

The Commission attempted to locate both published material that links misconduct risks with specific policing functions or policing powers as well as that that links misconduct risks policing roles in the intelligence and security areas.

Other than that which links corruption or misconduct opportunities with drug law enforcement, there is not a published body of work that has specifically looked at the linkages between specific types of police work or police powers and specific types of police misconduct. More generally, there is currently no developed taxonomy to classify functions of law enforcement or other types of organisations in terms of their level of corruption or misconduct risk (Gorta 2006, p. 209).

However, the Commission has reviewed available police corruption inquiries and other research material on police corruption and police misconduct to identify possible linkages that may be relevant to the work of the CTCC.

[11] The officers who nominated this risk did not consider it to be specific to the CTCC, but considered it to be a potential misconduct risk facing officers in many commands.

Misconduct risks associated with the work undertaken by the former Special Branch

Given the similarities in the nature of the work undertaken by the Special Branch and the CTCC, the reports of the Investigations by the Royal Commission and by this Commission into the operation of the Special Branch are of most immediate relevance. As discussed in Chapter 2 of this report, these investigations identified the following major failings of the operations of the former Special Branch:

- disregard of its charter and a lack of accountability
- information gathering on people who posed no threat of politically motivated violence or similar matters (inappropriate targeting) and the belief that it could be used for political advantage against persons on whom 'dirt files' had been kept
- an unacceptable overlap between the functions of information gathering and protection of VIPs, leading to information being held about VIPs and public figures, rather than those who posed a threat to them
- informant management and payment of informants
- poor record keeping practices and ineffective and outdated intelligence system
- poor supervision
- unsatisfactory recruitment practices.

While some of the CTCC officers who were interviewed identified 'officers acting outside of their charter' and 'informant management' as potential misconduct risks, it is noteworthy that these were not mentioned as misconduct risks in the CTCC's command-level response.

Political and community pressure associated with investigation of terrorism may lead to misconduct in investigation

Punch (2000) has commented on how pressure to produce results can lead to misconduct in investigations. He has used examples taken from the investigation of terrorist acts in Northern Ireland:

> The campaign of violence by the IRA in Britain led to a series of bomb explosions with many deaths and a large number of casualties. Several suspects, including the 'Birmingham Six' and the 'Guildford Four' received long prison sentences. Many years later doubts were raised about these convictions and in subsequent investigations it emerged that the suspects had been intimidated, statements and confessions had been falsified and tampered with, relevant material had been withheld from the court, and the forensic evidence was dubious. The successful appeals led to the release, after 16 years, of people who had been imprisoned unfairly and who had been victims of 'miscarriage of justice'.
>
> The pressure surrounding these cases of terrorist violence presumably fostered the justification that the convictions were so important that the detectives 'had to break the law' to secure them – 'noble cause

> corruption'. The difficulty with this rationalisation is that it was undermined when a second series of cases came to light where suspects in relatively minor cases had been 'set up' by the police (some of these suspects were particularly vulnerable people). If the IRA cases might have been justified in police minds as extreme and untypical then this new series of miscarriages hinted that rule-bending to secure a conviction was routine, wide-spread and employed against small fry (Punch 2000, pp. 309-310).

Similarly Prenzler has commented on the pressure to fabricate evidence in cases where there is political and community pressure to bring offenders to justice:

> Pressure to fabricate evidence comes from a number of sources including political and community pressure to bring offenders to justice – particularly for more terrifying or repugnant crimes. This can be exacerbated by the use of a crime 'clearance rate' as a police performance measure (Prenzler 2002, p. 14).

The HMIC has also written about the consequences of the pressures on police to 'perform well':

> One of the core activities of policing is to enforce the law, which often entails the investigation and prosecution of offenders. The pressure on forces to perform well, and demonstrate through high detection rates that they are doing so, has resulted in pressure on 'front line' service deliverers to 'trawl the margins' for elusive detections and generally find any way to improve the figures. Evidence was found of boundaries sometimes being pushed too far and unethical practices operating … (HMIC 1999, p. 3).

Misconduct risks identified in other police misconduct literature

Potential misconduct risks identified from the broader literature on police misconduct include risks in the areas of informant management and information handling. For example, the HMIC (1999), Punch (2000) and Miller (2003) have commented on the misconduct risks associated with the relationship between police officers and their criminal informants:

> In the context of a potential lack of integrity, the use of informants is possibly the highest risk area in the work of the modern Police Service … Her Majesty's Inspectorate is extremely concerned to discover that effective systems for ensuring informants are used with integrity either do not exist at all, or are ignored (HMIC 1999, p. 22).

> When the relations are close and cosy, police officers can come to share the world-view of criminals. This can readily happen in informant-handler relationships and undercover work (Marx 1988 cited by Punch 2000, p. 315).

> The vulnerable areas of police work are predictable – vice, drugs, undercover work, informant-handler relationships, licensing, and those responsible for placing contracts with companies. These areas require careful rotation of personnel after a number of years of exposure to danger zones (Punch 2000, p. 319).

> Problems with the relationships between police officers and criminal informants feature significantly within the types of internally-networked corruption outlined in the last chapter. One interviewee identified how problems could emerge from relationships with informants:
>
> > A bobby becomes the bosom pal of the informant … when the informant steps over the line the bobby covers for him.
>
> … Given the inherent risk that comes from police officers associating with those connected with crime, these relationships are likely to remain an important corruption risk (Miller 2003, pp. 20-21).

Unauthorised release of information is recognised as the most common and damaging type of police corruption in the United Kingdom:

> … information compromise represents the single most common type of [police] corruption activity. It can involve information from a range of police sources, including databases, files or documents, and word-of-mouth. Forms of compromise include obtaining information for personal purposes, passing information to friends and associates, leaks to the media, and deliberate leaks to criminals (Quinton & Miller 2003, p. 5).
>
> The major threats identified in respect of professional standards were information leakage, in particular using intelligence or information for personal gain or passing it on to associates; infiltration of the organisation, which is an increasing threat in the ever-widening 'police family'; and substance misuse, with its associated risks of coercion and targeting for blackmail (HMIC 2006, p. 9).
>
> In 2002, the Home Office published research on corruption within policing … the predominant perpetrators were lone staff members, and the main target was sensitive information (HMIC 2006, p. 104).

Potential misconduct risks identified by other law enforcement agencies carrying out similar functions

The Commission contacted several law enforcement agencies in other jurisdictions that conduct functions similar to those undertaken by the CTCC to request:

- information on the risks in their operation that could lead to misconduct
- any assigned levels of risk (for example, from very high to negligible) to the risk categories, and
- if possible, a brief note on their process for identifying risks.

In addition to information handling risks such as the loss of restricted information due to a lapse in security, the loss of restricted information on mobile devices or inappropriate access to sensitive or privileged information; other misconduct risks identified by one or more of these law enforcement agencies included:

- inappropriate collection of holdings – privacy violations
- inappropriate covert targeting, and
- informant management.

Review of complaints made against CTCC officers

As an additional method of identifying potential misconduct risks, the Commission examined the complaints made about officers working in the CTCC that were registered on C@tsi[12] between March 2003 and May 2006. The Commission did this to:

- identify misconduct allegation types to see whether these allegation types are similar to or different from allegations made about officers undertaking other types of police work
- determine whether any of the allegations made about CTCC officers were consistent with types of misconduct previously identified by the Royal Commission in relation to the former Special Branch.

The Commission's examination revealed that there was nothing to distinguish the types of allegations made about police officers assigned to the CTCC from allegations made about police officers assigned to other commands. Nor did the Commission find any examples of complaints that reflected the types of misconduct previously identified by the Royal Commission in relation to the former Special Branch.

[12] The NSW Police complaints management system.

Table 6.1: Summary of potential misconduct risk areas identified through different sources of information

Potential misconduct risk area	Identified in CTCC command-level written response[13]	Identified in interviews with key CTCC officers[14]	Identified in investigations of former Special Branch	Identified by other law enforcement agencies	Identified from the literature
Unauthorised release or misuse of information*	√	√	X	√	√
Inappropriate storage of information*	√	√	√ [15]	√	X
Inappropriate collection of information*	√	√ [16]	√ [17]	√	X
Recruitment of officers for information by external agencies (national security issue)*	√	√	X	X	X
Improper associations*	√	√	X	X	X
Misuse of motor vehicles*	√	√	X	X	X
Misuse of mobile phones*	√	√	X	X	X
False overtime claims*	√	X	X	X	X
Misuse of covert licences*	√	X	X	X	X

[13] These misconduct risks were provided in the command-level response in a letter from NSW Police Deputy Commissioner Specialist Operations to Commissioner Police Integrity Commission dated 20 April 2006, received 20 April 2006.

[14] These misconduct risks were identified by key CTCC and PORS officers interviewed in March-April 2006.

[15] The Royal Commission referred to 'lax and inconsistent record keeping practices' and 'the ineffective and outdated intelligence system [Special Branch] maintained (Wood 1997, p. 251).

[16] Those interviewed worded this as 'improper targeting of suspects'.

[17] The Royal Commission referred to 'the opening of dossiers and the keeping of records in respect of various persons, for example, barristers practising in the criminal law who on no reasonable basis could have been of interest to Special Branch within its charter' and 'the belief that it had long been associated with political interests, and seen as an agency which could be used for political advantage against person on whom 'dirt files' had been kept' (Wood 1997, p. 251).

* Wording of these potential misconduct risks is taken directly from CTCC command-level written response.

Table 6.1 (continued)

Potential misconduct risk area	Identified in CTCC command-level written response[18]	Identified in interviews with key CTCC officers[19]	Identified in investigations of former Special Branch	Identified by other law enforcement agencies	Identified from the literature
Compromise in, or impropriety of, investigation	X	√	X	X	√ [20]
Informant management	X	√	√	√	√
Officers act outside their charter	X	√	√	X	X
Covert search warrants	X	√	X	X	X
Security of exhibits/exhibit handling	X	√	X	X	X
Drug and alcohol abuse	X	√ [21]	√ [22]	X	X

[18] These misconduct risks were provided in the command-level response in a letter from NSW Police Deputy Commissioner Specialist Operations to Commissioner Police Integrity Commission dated 20 April 2006, received 20 April 2006.

[19] These misconduct risks were identified by key CTCC and PORS officers interviewed in March-April 2006.

[20] Discussed in the literature as occurring as a result of pressure to produce results (HMIC 1999, p. 3; Punch 2000, pp. 309-310; Prenzler 2002, p. 14).

[21] The officers who nominated this misconduct risk did not consider it to be specific to the CTCC, but considered it as a potential misconduct risk facing officers in many commands.

[22] The Royal Commission did not specifically refer to drug and alcohol abuse. It referred to 'long lunches by supervisors and the consumption of alcohol on duty, particularly within the Special Branch office where it seems a bar was regularly opened in the afternoons (Wood 1997, p. 251).

Potential misconduct risks identified from prosecutions of terrorism suspects

The Commission used comments made in the judgment on three pre-trial motions concerning the admissibility of evidence in *Regina v Zaky Mallah*[23] as an additional source to identify potential misconduct risks. The judgment revealed that correct procedures had not been followed in this instance when NSW Police did not obtain a Controlled Operations Certificate from the outset of an undercover aspect of the operation (though a Controlled Operations Certificate was subsequently obtained).

In this case the failure appeared to be the result of a lack of knowledge about proper procedures regarding the use of police powers. Evidence on which this judgment was based portrayed some officers not being aware of the legislation and procedures required when conducting the investigation and not taking steps to find out more or to obtain legal advice. It is of concern that senior officers involved in the Mallah investigation were not aware of the required procedures in relation to Controlled Operations. Moreover, these officers said they did not take steps to remedy this situation by either reading the legislation or seeking legal advice. Instead they said they acted on their 'assumptions' and 'beliefs' (Judgment in R. v Zaky Mallah, pp. 27, 39). This is of particular concern given that the amount of legislation that officers are required to be familiar with has increased as a result of the additional police powers provided to counter terrorism in NSW (refer to Chapter 3 and Appendix 3 for further information about this legislation).

This example both highlights operational risks for the CTCC where officers may not be aware of the appropriate procedures and identifies the possibility of officers who are aware of the appropriate processes failing to follow them.

[23] R-v-Mallah [2005] NSWSC 358 (11 February 2005).

6.3 SUMMARY OF KEY POINTS

1. The work of the CTCC encompasses many of the same functions that were undertaken by the Special Branch and the PSG. Hence it would be incorrect to argue that the risks and oversight arrangements required for the CTCC should be different from those of the former PSG based on any differences in their functions.
2. The work of the CTCC is broader than counter-terrorism policing. Much of its work is covert, though it can become high-profile. The CTCC's work has a preventative focus. The nature of the work may cause some people to fear the creation of 'dirt files', even if this fear is misplaced. The work requires cooperative, coordinated and consultative relationships with officers from a range of federal and state agencies. The structure has been subject to continuing change.
3. Within NSW Police, misconduct risk identification occurs at the command level rather than the corporate level. At the corporate level, NSW Police was unaware of any misconduct risks specifically facing officers working in the CTCC being identified and documented.
4. There is no consolidated list of the misconduct risks that might face officers working in the CTCC.
5. While there was overlap between the potential misconduct risks provided in the CTCC's written response and the misconduct risks nominated by key CTCC officers who were interviewed, the lists were not the same. Both the CTCC's written response and the officers' interview responses identified the following potential misconduct risks:
    - Unauthorised release or misuse of information – either deliberately or accidentally – especially information provided from third parties
    - Inappropriate storage of information
    - Inappropriate collection of information
    - Recruitment of officers for information by external agencies (national security issue)
    - Improper associations
    - Misuse of motor vehicles, and
    - Misuse of mobile phones.

    In addition the CTCC's written response included the following two potential misconduct risks that were not mentioned by any of the key CTCC officers interviewed: 'False overtime claims' and 'Misuse of covert licenses'.

    Key CTCC officers who were interviewed also identified the following potential misconduct risk areas: 'Compromise in, or impropriety of investigation', 'informant management', 'officers acting outside their charter', 'covert search warrants', 'security of exhibits/exhibit handling', and 'drug and alcohol abuse'.
6. The CTCC command-level response did not include 'informant management' or 'officers acting outside their charter' both of which had been documented to be problems experienced by the former Special Branch.

7. TREATING THE MISCONDUCT RISKS

This chapter describes the strategies that the CTCC has advised that it uses to treat the misconduct risks it has identified, as well as the strategies that it has in place to minimise the possibility of the CTCC repeating the failings of the former Special Branch.

Strategies that were reported as being used by the former PSG, which are not reported as being currently used by the CTCC, are also documented in this chapter.

7.1 BACKGROUND

There are different ways of treating or responding to risks including:

- risk avoidance
- risk reduction, that is reducing the likelihood of the risk occurring, its consequences if it does occur, or both its likelihood and its consequences
- risk sharing, or
- acceptance of the risk.

Decisions on how best to respond to misconduct risks and how to establish controls need to consider the relative costs and benefits.

According to the Australian/New Zealand Risk Management Standard, 'risk treatment involves identifying the range of options for treating risks, assessing these options and the preparation and implementation of treatment plans' (Standards Australia & Standards New Zealand 2004, p. 20).

7.2 TREATING MISCONDUCT RISKS IDENTIFIED BY THE CTCC

SOURCES OF INFORMATION

The Commission obtained information about the CTCC's misconduct risk treatment strategies from three sources:

- the CTCC's command-level written response to the Commission's questions
- the interviews Commission staff conducted with key CTCC officers, and
- an examination of the copies of the CTCC's CMF templates that the CTCC had provided to the Commission.

In its written questions to the CTCC, after seeking information on the misconduct risks that have been identified, the Commission asked, 'for each of the identified

misconduct risks what strategies are in place for reducing or managing this misconduct risk?'. It also asked for each risk whether any additional strategies were proposed.

In the interviews held with key CTCC staff in March/April 2006, officers were asked to identify what they considered to be the major misconduct risks. In each case, the officers were asked to describe the strategies currently in place for managing the risk. Officers were also asked what additional strategies might be useful in managing each risk. It should be noted that each officer who was interviewed described risk treatment strategies only for those misconduct risks that he had identified. Hence not all nine of the misconduct risks that were identified in the command-level response were discussed in the interviews.

Table 7.1 summarises the risk treatment strategies for each of the nine misconduct risks that had been identified in the written command-level response (see Section 6.2 of Chapter 6). In this table, the misconduct risk treatment strategies provided in the command-level written response are presented separately from the strategies described in the interview responses, which in turn are presented separately from the treatment strategies identified from the CTCC's CMF templates.

STRATEGIES IN PLACE

As outlined above, in its written questions the Commission asked the CTCC 'for each of the identified misconduct risks, what strategies are in place for reducing or managing this misconduct risk?'. Rather than providing a separate response for each of the different misconduct risks, the CTCC provided the following aggregated response:

- Command Management Framework
- Auditing
- Dip sampling auditing and CMF processes
- Operations Review Committee
- Rotation of staff in and out of Command
- Rotation of staff within Dignitary Protection Unit so that case officers and coordinators do not remain consistently allocated to one country etc
- Supervision
- Staff education/awareness.[24]

Where possible, in Table 7.1 the Commission has attempted to subdivide the CTCC's aggregated response and to allocate treatment strategies to each of the misconduct risks.

The CTCC did not provide any consolidated documentation of its risk treatment strategies. When the Commission requested a copy of 'any documentation of the misconduct risks as being faced by officers working in the CTCC (Q10), as well as

[24] The command-level responses described in this chapter are taken from a letter from NSW Police Deputy Commissioner Specialist Operations to Commissioner Police Integrity Commission dated 20 April 2006, received 20 April 2006.

any available information concerning the assessment (Q11) and the management of these misconduct risks (Q12), the CTCC responded that 'there is no consolidated document'.

In interviews some officers identified additional misconduct risks to those that were identified in the command-level written response. These additional misconduct risks and the associated treatment strategies identified in interviews with key CTCC officers are listed in Table 7.2.

From Tables 7.1 and 7.2, it can be seen that the treatment strategies described by the CTCC encompass a range of different methodologies including:

- physical security (such as keypad controls on rooms)
- use of corporate information systems with built-in audit capacity
- decision making concerning information collection by a group (Operations Review Committee) rather than by an individual
- supervision and record keeping in relation to investigations
- rotation of officers, and
- audits both to deter and to detect individual examples of misconduct.

From its examination of the CTCC's CMF templates that were provided, the Commission was unable to find any clear link between any of the four misconduct risks that the CTCC assessed as 'moderate' and strategies listed in the CTCC's CMF. Similarly the Commission was unable to find any clear link between three of the five misconduct risks that the CTCC assessed as 'minor' and strategies listed in the CMF templates provided.

In the interviews, some officers described broader strategies which would be likely to be aimed at managing a number of misconduct risks. Such broader risk treatment strategies included:

- integrity checks that are conducted on all staff who come to the CTCC, and
- an induction process that specifies expectations of staff working in the CTCC.

Table 7.1: Treatment strategies described for identified misconduct risks

Misconduct risk identified in CTCC command-level written response	Risk treatment described in command-level written response[25]	Risk treatment described in responses given by key CTCC staff who were interviewed[26]	Treatment outlined in CMF [27]
Unauthorised release or misuse of information – either deliberately or accidentally (assessed as a 'moderate' risk by the CTCC)	• Auditing	• Regular audits of access to COPS and similar audit of material of access to ASNET (Australian Secure Network). • Do not print unnecessary copies of material. • All staff have 'secret' clearance at a minimum. • Shredders rated to take secret material. • Keypad controls to Internet room, ASNET room, Records Room that provide records of who access the room and when they access it. • All disseminations are made by the Commander CTCC. • Log maintained for what information is disseminated by the Command. • All staff have signed confidentiality agreements.	None identified in CTCC's CMF templates*

[25] Based on letter from NSW Police Deputy Commissioner Specialist Operations to Commissioner of the Police Integrity Commission dated 20 April 2006. The Commission has attempted to allocate treatment strategies for each of the misconduct risks from the CTCC's aggregated response.

[26] Based on responses to interviews conducted in March-April 2006 with Assistant Commissioners Counter Terrorism and Public Order Management (2 individuals), Commander CTCC, CTCC unit leaders and PORS Commander.

[27] Based on copies of the CTCC's CMF templates provided in correspondence from the Assistant Commissioner Counter Terrorism and Public Order Management to the Director Intelligence and Executive Services of the Police Integrity Commission, dated 26 June 2006.

* No relevant treatment strategy for this misconduct risk was able to be identified by the Commission from the CTCC's CMF templates provided on 26 June 2006.

Misconduct risk identified in CTCC command-level written response	Risk treatment described in command-level written response[25]	Risk treatment described in responses given by key CTCC staff who were interviewed[26]	Treatment outlined in CMF [27]
Inappropriate storage of information (assessed as a 'moderate' risk by the CTCC)	Auditing	• National Classified information is held on ASNET (Australian Secure Network) and stored in B-class safes. All other information is stored in corporate systems (e.g. COPS, e@gle.i). • Only retain information on corporate systems. These systems are subject to audit. All information is entered on COPS, where information is entered as stand alone entries (e.g. Person X is engaging in Y). • There is greater oversight of all information received by the CTCC than information in any other command because all information is considered and managed by the Operations Review Committee (ORC).	None identified in CTCC's CMF templates*
Inappropriate collection of information (assessed as a 'moderate' risk by the CTCC)	• Target selection compared against charter and mission of Command • Operations Review Committee (ORC)	• Have intelligence collection plan, with the information collected solely focussed on politically motivated violence. • Investigations are instigated through the ORC process and threat assessment process to ensure that officers are not doing frivolous investigations. Investigations are initiated on basis that a criminal offence has been or is going to be committed. • Management of information by the ORC means that decisions are made by a panel of people, not all of whom are involved in a job, rather than being decided by an individual. When ORC decides information should be further investigated, the investigations go back to the ORC for further discussion as to whether it should be continued and recommendations for further action.	None identified in CTCC's CMF templates*

Misconduct risk identified in CTCC command-level written response	Risk treatment described in command-level written response[25]	Risk treatment described in responses given by key CTCC staff who were interviewed[26]	Treatment outlined in CMF [27]
		• No investigation is commenced without approval of Unit Leader and Commander. • Relationship with other agencies such as AFP and ASIO brings with it additional controls. i.e. the conduct of NSW Police officers is subject to being observed by the officers from the other agencies with whom they work, - e.g. an AFP officer might ask 'why are you working on X when you should be working on Y?'	
Recruitment of officers for information by external agencies (national security issue) (assessed as a 'moderate' risk by the CTCC)	• Rotation of staff within Dignitary Protection Unit so that case officers and coordinators do not remain consistently allocated to one country etc.	• Rotate officers through activities and duties so that do not have the same staff member always doing the consular visits at the one consulate or continuing to work with the same dignitaries. • Supervisors get to know their staff. Through performance management interviews with staff, proactive interviewing to identify HR and operational issues. • Regular training days, meetings with staff, reinforce strict doctrine of manner in which they do their jobs and unit leader's expectations. Staff are aware that any breach would mean that they would be transferred. • Remind everyone of their obligations in terms of confidentiality. • Discuss all aspects of operations at team leader level, so know when an officer is going to talk to suspect, make sure such information in logged in note books. • Regular COPS audits on what officers are looking at	None identified in CTCC's CMF templates*

Misconduct risk identified in CTCC command-level written response	Risk treatment described in command-level written response[25]	Risk treatment described in responses given by key CTCC staff who were interviewed[26]	Treatment outlined in CMF [27]
Improper associations (assessed as a 'minor' risk by the CTCC)	(Same treatment strategies as above)	(Same treatment strategies as above)	None identified in CTCC's CMF templates*
Misuse of motor vehicles (assessed as a 'minor' risk by the CTCC)	• Command Management Framework • Auditing	• Checks of motor vehicles	• Vehicle diaries checked weekly to ensure compliance with NSW Police policy and procedures re use of vehicles. Vehicle diaries also checked against roster/duty books.
Misuse of mobile phones (assessed as a 'minor' risk by the CTCC)	• Command Management Framework • Auditing	• Audits of mobile phones	• Mobile Telephone Register is checked quarterly and endorsed monthly by the Supervisor to ensure all items including handsets and SIM cards are accounted for. • Mobile Telephone accounts are checked by the users and endorsed to ensure that they are used as per Command SOPs. • Unit leader to endorse the mobile telephone accounts to ensure appropriateness and proper usage.

Misconduct risk identified in CTCC command-level written response	Risk treatment described in command-level written response[25]	Risk treatment described in responses given by key CTCC staff who were interviewed[26]	Treatment outlined in CMF [27]
False overtime claims (assessed as a 'minor' risk by the CTCC)	• Auditing	Although 'false overtime returns' were not specifically mentioned, some officers raised what they referred to as 'normal supervisory issues' and mentioned the following: • checks of rosters • checks of duties • audits of diaries • day-to-day management and supervision of staff including 'intensive supervision' where supervisors attend the work sites at unannounced times.	None identified in CTCC's CMF templates*
Misuse of covert licences (assessed as a 'minor' risk by the CTCC)		(This risk was not discussed by the key CTCC officers interviewed.)	None identified in CTCC's CMF templates*

Table 7.2: Additional misconduct risks and associated risk treatment strategies identified in interviews with key CTCC officers

Additional misconduct risks identified in CTCC interviews	Risk treatment described in responses given by key CTCC staff who were interviewed
Compromise of, or impropriety in, investigation	• Investigations are recorded in the corporate e@gle.i system. This system incorporates a range of checks and balances – such as terms of reference, investigation plan enables monitoring, statistics on numbers of statements taken by different officers during a period. • There are layers of review – through Inspectors, Superintendent reports on a regular basis to Assistant Commissioner, also conduct regular reviews with NSWCC. • Special facets of investigations are subject to checking processes, e.g. if doing telephone intercept or listening device need to obtain order from a Supreme Court judge. • CTCC conducts a post-operational assessment.
Informant management	• Informants/community contacts are referred to as 'sources' and are managed using the NSW Police Source Management Policy.
Officers act outside their charter	• Have regular meetings where 'staff regularly hear what they are about'. • CTCC has much clearer tasking than there was 10 years ago, with stringent audit trails for who does what and how long it takes on e@gle.i. Also corporate systems (e.g. COPS, SOURCE) have built-in audit trails • Relationship with other agencies such as AFP and ASIO brings with it additional controls, i.e. conduct of NSW Police officers is subject to being observed by officers from other agencies with whom they work. • Every project starts with an assessment that is transparent, steps of the investigation are monitored and then there is a post-operational review. • Officers are aware that they may have to give evidence in court and their work is subject to further checks and balances in terms of judicial review.
Covert search warrants[28]	• Standard Operating Procedures in place. • Video tape search • Have an independent observer • Oversight by the Ombudsman's Office through information provided consistent with memorandum of understanding

[28] The CTCC provided a copy of its Standard Operating Procedure (SOP) for covert search warrants. This SOP provides for the inclusion of 'an independent observer (where practicable)' and a 'video officer (where practicable)'. .It specifies that the Independent Officer, 'where possible, to be of the rank of Inspector or above, and is not to be directly connected or associated with the investigation for which the warrant is sought'.

Table 7.2 (continued)

Additional misconduct risks identified in CTCC interviews	Risk treatment described in responses given by key CTCC staff who were interviewed
Security of exhibits/exhibit handling	• CTCC does not hold its own exhibits, they are held in the relevant local area command. However, it is still of concern that exhibits are identified and recorded correctly. • Have Standard Operating Procedures. Use corporate exhibit handling processes that involve having an exhibits officer, recording exhibits in record book, videotaping of search.

PROPOSED STRATEGIES

In addition to the risk treatment strategies that the CTCC has advised are currently in place (see Tables 7.1 and 7.2), in its written response the CTCC has said that it proposes to conduct risk assessments:

> on every officer attached to the Command, utilising general policing risk factors and in addition factors such as previous complaints for release of information, inappropriate association. This will enable identification of officers at risk and allow the Complaints Management Team to devise and implement strategy to manage those individual risks.

The development of a risk profile of the individuals working in the command was also mentioned by several officers in the interviews that were conducted by Commission officers.

Other possible risk treatment strategies that were proposed in the interviews by one or more officers included:

- obtaining advice as to how other agencies (such as the Commission, the Ombudsman's Office and the State Crime Command) identify and manage their misconduct risks
- seeking advice on the method that the State Crime Command uses for target selection, and
- regularly reviewing misconduct risks and their management.

MONITORING THE EFFECTIVENESS

The Commission asked the CTCC: 'Does the CTCC monitor the effectiveness of the treatment strategies it uses to reduce or manage individual misconduct risks? If so, could you please provide any available documentation that helps illustrate the way this monitoring is undertaken?'. To this the CTCC responded:

- CMF framework

- Complaints Management Team meeting minutes recorded on CATSI
- Local Management Issues
- Conduct Management Plans (if required).

The CTCC's response did not elaborate further on how it monitors the effectiveness of its treatment strategies. From the information provided to the Commission, it is not possible to assess the effectiveness of the individual misconduct risk treatment strategies used by the CTCC.

7.3 STRATEGIES TO MINIMISE THE LIKELIHOOD OF REPEATING THE FAILINGS OF THE FORMER SPECIAL BRANCH

In both its written questions to the CTCC and the questions asked during the interviews with key CTCC officers, the Commission specifically sought information about the strategies the CTCC uses to minimise the likelihood of repeating the failings of the former Special Branch. In particular, the Commission sought information concerning strategies in place regarding those practices which had been specified in Section 16 of the *Police Act 1990* to be examined in the annual audits of the PSG. The Commission also sought information on the CTCC's recruitment practices. In other words, the Commission sought information concerning strategies to minimise the likelihood of:

- disregard of its charter and a lack of accountability
- inappropriate target selection and information collection
- inappropriate informant management and payment of informants, and
- unsatisfactory recruitment practices.

In summary, the responses provided indicate that rather than using its own systems, wherever possible the CTCC uses NSW Police corporate systems, some of which incorporate facilities that enable regular audits to be conducted.

ADHERENCE TO CHARTER AND ACCOUNTABILITY

When asked to identify what mechanisms are in place to ensure that it does not disregard its charter or established role and functions, the CTCC identified the following mechanisms:

- Investigations are conducted within the confines of the National Counter Terrorist Plan (National Counter Terrorist Committee)
- Target selection assessed by Intelligence Unit and approved and monitored through Operations Review Committee
- Investigations are directed by approved investigations plans
- Intelligence Collection is directed by an approved Intelligence Collection Plan
- Oversight by the New South Wales Crime Commission Operational Committee

- Huntley Reference document (NSWCC) outlining the parameters within which investigations are conducted under the auspices of the New South Wales Crime Commission
- Regular operational reporting of investigations with reports recorded in an accountable, auditable, corporate systems – Eaglei, TRIM, COPS and Source
- Management meetings
- Command Management Framework
- Complaint Management Team
- Use of corporate systems – COPS/Source/Eaglei/TRIM
- Management & supervision of staff.

In response to the question, 'what mechanisms are in place to ensure that the work of the CTCC is accountable', the CTCC responded:

- Command Management Framework
- Management meetings
- Command meetings
- Availability for [NSW Police] audit
- Use of corporate computer systems wherever possible.

TARGET SELECTION AND INFORMATION COLLECTION

In response to the Commission's question, 'what mechanisms are in place to ensure ethical target selection, collection, storage and use of intelligence', the CTCC provided the following list:

- Use of corporate systems – COPS/Source/Eaglei/TRIM
- All intelligence reports recorded via COPS
- TRIM system used to record intelligence taskings
- All sources entered on the Source system and Source Management policies adhered to
- Target selection compared against charter and mission of Command
- Operations Review Committee
- NSW Crime Commission meetings.

INFORMANT MANAGEMENT

When asked about informant management, the officers who were interviewed were consistent in their responses. They each said that informants and community contacts are both referred to as 'sources' and are managed using the NSW Police Source Management Policy and the related corporate systems.

RECRUITMENT

Risks relating to recruitment were also specifically probed in the structured interviews, because they had previously been raised by the Commission and the Royal Commission in relation to the former Special Branch. Officers who were interviewed each said that recruitment is determined on merit and is open to everyone within NSW Police who is appropriately qualified (e.g. in intelligence, investigations - depending on the nature of the vacant position). The recruitment process was described as including the following:

- all positions are advertised on state-wide basis
- formal committees are in place to select on merit
- reports are received from current supervisors of officer as well as current commander
- applicants are short-listed
- recommendations are made to Commander of the CTCC
- integrity checks are conducted by Professional Standards Command
- those appointed to the CTCC are subject to National Security vetting.

One officer who was interviewed stated that the CTCC has a policy of 3-5 years tenure. However, given that the CTCC commenced in 2003, this has not yet been an issue. He suggested that the command may need to revisit this policy in terms of potential loss of expertise if tenure is capped at a five-year period.

The appointment of the current Commander of the CTCC, who had never previously worked in the CTCC or PSG, was provided as an example that the current procedures do not lead to a 'closed shop' approach to recruitment.

7.4 PREPARING CTCC OFFICERS FOR THE MISCONDUCT RISKS THEY MIGHT FACE

In educational materials prepared for the Royal Canadian Mounted Police, Gilmartin has emphasised the importance of officers being well-prepared for ethical dilemmas before they face them:

> Officers live and work in a constantly changing and dynamically social context in which they are exposed to a myriad of ethical conflicts. When either unprepared or unaware, officers are more likely to 'go with the flow' than they would be if adequately prepared to face potentially ethical risks. Everyday, officers practice mental preparation as it relates to tactical situations. Officers who are mentally prepared to face a lethal encounter are more likely to be successful than officers who are tactically proficient but mentally unprepared. Just like lethal encounters, ethical dilemmas occur at the most inopportune times, frequently without warning and with little time to stop and think about the situation. When inadequately prepared, even the most honest, above reproach officers can make inappropriate split-second ethical decision … If officers are going to survive ethical dilemmas, they need to be as mentally prepared as they would be for tactical encounters (Gilmartin 2003, p. 125).

In the same way, it can be argued that it is important to prepare officers for the misconduct risks that they might face as part of their work, prior to the officer actually facing these risks. For this reason the Commission considered the nature of the information provided to the CTCC officers concerning the misconduct risks that they might face.

INFORMATION PROVIDED BY NSW POLICE AT THE CORPORATE LEVEL

When asked whether NSW Police provides any information or training to officers about the misconduct risks they are likely to face in their work and how best to manage these risks, NSW Police's response to the Commission focussed on the generic information provided to all officers, rather than information concerning the specific risks associated with undertaking different types of policing work in different commands. For example, NSW Police informed the Commission that the topic of misconduct 'is woven through the subject [PPP123 undertaken by students of policing] and associated assessment items'. A further example given by NSW Police was that the Professional Standards Command initiates numerous publications for dissemination through media such as the Police Service Weekly and the intranet, 'these address a broad range of issues including drink driving, improper associations, drug use and complaints environment, off duty conduct, and, conflicts of interest'.

INFORMATION PROVIDED BY THE CTCC AT THE COMMAND LEVEL

In its written questions to the command, the Commission asked what, if any information has been given to staff of the CTCC about the misconduct risks that they are likely to face in their work and how best to manage these risks. The CTCC responded that 'it is currently being considered to include identified misconduct risks in induction documentation'.

The Commission also asked whether the CTCC has any misconduct prevention strategies that are specific to the CTCC (and if so, what are these strategies and how does the CTCC internally publicise its misconduct prevention strategies), the CTCC responded

- The CMF is tailored to the requirements of this particular Command
- The principle of the CMF is that it is practised by officers at each level of the Command, therefore allows each officer to take part in the monitoring, reporting and compliance of risk.

In their interview responses, some CTCC officers mentioned that staff are provided with an induction document that communicates expectations held of those who work in the CTCC. Some also mentioned that when issues arise and are recognised through the CMT (such as inappropriate use of computers) a reminder email is sent to all staff concerning appropriate practices.

THE CTCC INDUCTION PROGRAM

The CTCC's documentation of its Induction Program describes the command as unique and describes accountability and ethical professional self regulation as being fundamental to all facets of the command's responsibilities:

> The Counter Terrorist Co-Ordination Command is a unique command within the New South Wales Police Service. …
>
> Fundamental to all facet's of the command's responsibilities and activities is personal accountability and ethical professional self-regulation. The command operates with a philosophy of high trust in which excellence and diligence are promoted. The command fosters a workplace culture where there is zero tolerance of corruption and which strives for excellence. …
>
> The management team within the Command appreciates that how we achieve is as important as what we achieve, to this end the ethical collection, evaluation and dissemination of information within this Command is ensured by a series of Command specific risk management practices (NSW Police Service (undated), p. 4).

The 'Command specific risk management practices' referred to in the last paragraph quoted above do not appear to be described in the material that follows within the documentation of the Induction Program.

The CTCC induction program does not refer to or acknowledge the documented failings of the former Special Branch. Nor does it refer to the former PSG.

In terms of information collection, guidance is provided on where within the NSW Police 'COPS' data system to store different types of information. The Intelligence Unit Leader's responsibility for the 'ethical storage' of intelligence holdings is referred to, but not explained; and new staff are alerted to the fact that their access to COPS will be audited on a regular basis:

> Responsibilities of Staff
> Intelligence Unit Leader is responsible for the oversight and quality review of all intelligence holdings of the CTCC along with the day to day maintenance of COPS intelligence holdings including; evaluation, annual review and ethical storage.
>
> Audit
> Cops audits will be conducted on a regular basis using CMF (NSW Police Service (undated), p. 11).

While the CTCC's mission statement and principal roles are documented in the Induction Program, no explicit reference is made to the CTCC's charter. Nor is any explicit reference made to that part of the charter that specifies limits to the range of intelligence activities and investigations that the CTCC should undertake:

> The CTCC is to ensure that intelligence and investigatory operations are limited to persons who are reasonably suspected of terrorist acts, and the CTCC shall not conduct investigations of persons solely on the basis of political views, except to the extent that the expression of those views may constitute crimes (NSW Police Counter Terrorist Co-ordination Command Charter 2003, p. 1).

7.5 PROTECTIVE SECURITY GROUP CORRUPTION PREVENTION PLAN

The former PSG had its own documented 'Corruption Prevention Plan' (NSW Police Service 2000, pp. 16-23). This Corruption Prevention Plan was subdivided into the following nine strategies:

- Identify and focus on specific environmental risks relative to corrupt or unethical behaviour and conduct regular compliance and system audits to reduce potential for corrupt behaviour
- Monitor computer accesses across the command
- Promote an environment through the Professional Standards Council whereby staff are encouraged to discuss ethical dilemmas and best practice behaviour
- Improve understanding of professional behaviour as set out in the NSW Police Service Code of Conduct and Ethics and ensure understanding of required standards of behaviour and performance are well known and implemented
- Identify individuals or groups within the command deemed as being of high risk to corrupt practices and monitor these individuals or groups
- Ensure the collection, retention, dissemination and disposal of documentation is in accordance with the PSG Charter
- Educate all PSG personnel and enforce strict compliance with the Informant Management Plan
- Continually evaluate operational procedures relating to the Protective Security Group with a view to establishing best practice procedures and ongoing improvement to standard operating procedures, and
- Ensure probity in purchasing, accounts, payments, travel and subsistence expenses.

For each of these strategies, a number of tasks were identified. For each task a 'target/measure', responsible officer and review period were specified. For example, under the strategy 'ensure the collection, retention, dissemination and disposal of documentation is in accordance with the PSG Charter' the following tasks were itemised:

- Identify the number of sensitive targets[29] authorised by PSG Management Committee
- Audit on ASNET dissemination
- Audit information dissemination
- Audit ASIO requests for criminal records checks
- Random checks on security of documents to ensure appropriate security of confidential information

[29] 'Sensitive target' was defined as (1) Australian High Office Holders, and/or (2) An individual or group about whom it could be reasonably expected would generate wide spread media reporting if known (NSW Police Service 2000, p. 14).

- Audits on information holdings to ensure compliance with legislation and Police Service policy on retention and disposal of same
- Random audits on PSG information holdings, both hard copy and COPs to ensure compliance with PSG Charter (NSW Police Service 2000, p. 21).

The Commission was informed that the CTCC does not have a documented Corruption Prevention Plan or a Corruption Resistance Plan. The Commission was informed that corruption resistance was built in overall within the CTCC's CMF.

When asked whether the CTCC has any misconduct prevention strategies in place that are specific to the CTCC, the CTCC responded that its CMF is tailored 'for the requirements of this particular Command'.

7.6 OBSERVATIONS

The former Special Branch had been described as seeming 'accountable only to itself' (Wood 1997, p. 251), using 'anachronistic and unreliable' filing systems, and having 'no satisfactory procedures for the management of informants' (Police Integrity Commission 1998, p. 29). By using NSW Police corporate systems for information storage and source (informant) management, the CTCC has endeavoured to ensure that such criticisms are not applicable to its practices.

The CTCC has advised that it uses a range of strategies to manage the potential misconduct risks its officers may face. These strategies include: physical security measures, use of corporate systems for information management and informant management, a panel rather than individuals to decide which information should be collected, supervision and record keeping in relation to investigations, rotation of officers, and audits to deter and detect individual instances of misconduct. The CTCC has also advised that because its officers work closely with officers from other agencies such as the AFP and ASIO, the work of CTCC officers is subject to being observed by officers from the other agencies with whom they work.

While the adoption of such measures is likely to assist in minimising future misconduct, from the information provided to the Commission it is not possible to assess the effectiveness of the CTCC's misconduct risk treatment strategies. For example, in its written response the CTCC has not linked its treatment strategies to specific misconduct risks. Hence it has not clarified whether it has strategies in place for each of the misconduct risks it has nominated or whether it has decided that some of the misconduct risks do not require a specific response.

Although the Commission has been informed that the CTCC's CMF is tailored for the requirements of this particular command, the criteria used to tailor the CMF are not clear. If the CMF is to be a command risk management tool, it is perhaps surprising that there was no clear link between the CMF and any of the misconduct risks that the CTCC rated as 'moderate'. On the other hand, the CMF does include risk treatment strategies for misuse of motor vehicles and misuse of mobile phones (two of the five misconduct risks that the CTCC rated as 'minor').

While the CTCC described the strategies it uses to treat its misconduct risks, it did not provide any information about the range of options that had been considered, the

processes used to weigh possible different treatment options and/or why it chose its current treatment strategies. For example, the material provided to the Commission does not indicate whether or not the CTCC has considered using strategies such as those itemised in the former PSG's Corruption Prevention Plan, such as:

- identifying the number of sensitive targets authorised by the ORC
- conducting random audits on information holdings, both hard copy and COPS, to ensure compliance with the charter
- auditing ASNET disseminations
- conducting random checks of the security of documents to ensure appropriate security of confidential information.

Currently little is done to prepare CTCC officers for the specific misconduct risks they may face which are associated with the work of the CTCC. While the CTCC has advised that it is considering including identified misconduct risks in induction documentation, at the time of drafting this report CTCC officers were not told of the specific misconduct risks they might face in their work nor were they told of the problems identified in the way the former Special Branch conducted functions not dissimilar to those performed by the CTCC. No explicit reference is made to the CTCC's charter in its induction program. Nor is any explicit reference made to that part of the charter that specifies limits to the range of intelligence activities and investigations that the CTCC should undertake.

It would seem reasonable to expect that in circumstances where a high level governance document is in place for a business unit - such as a charter - that those aspects that establish standards for the conduct of staff should be cascaded down to systems and procedures that govern the day-to-day activities of staff, such as an induction program. However, based on the information obtained by the Commission during the course of this project, it would seem that the CTCC charter - which establishes a command-level standard requiring staff to ensure they do not investigate persons solely on the basis of political views - is not replicated in any of the misconduct risk management strategies identified by the command. This raises questions about the extent to which the charter can be regarded as effective in establishing standards at a high level for the CTCC and further illustrates the disconnected nature of the CTCC's approach to the management of misconduct risk.

7.7 SUMMARY OF KEY POINTS

1. Unlike the former Special Branch, the CTCC is not relying on stand-alone systems. Its systems are as accountable and transparent as the systems used by other NSW Police commands because it is using the same corporate systems.
2. The CTCC has advised that it uses a range of strategies to manage the potential misconduct risks its officers might face. From the information provided, it is not possible to assess the effectiveness of the CTCC's misconduct risk treatment strategies.
3. The information provided by the CTCC has not linked its treatment strategies, or its CMF, to the specific misconduct risks that it has identified in its written response. Hence it is not clear whether or not the CTCC has strategies in place for each of the misconduct risks it has identified.
4. The former PSG had a Corruption Prevention Plan, the material provided by the CTCC does not indicate whether or not the CTCC has considered using strategies such as those itemised in the former PSG's Corruption Prevention Plan.
5. CTCC officers are not told of the specific misconduct risks they might face in their work. Nor are they told of the documented problems associated with the way the former Special Branch discharged functions not dissimilar to those performed by the CTCC.

8. OVERSIGHT PROVIDED

This chapter compares the oversight previously required of the operation of the PSG with that currently in place for the CTCC. It also provides the views of key CTCC staff about the benefits as well as the disadvantages of the previous PSG oversight regime and their views of the monitoring or oversight required to adequately manage potential misconduct risks facing the CTCC.

8.1 BACKGROUND – OVERSIGHT OF THE OPERATION OF THE FORMER PSG

As outlined in Chapter 2, the former PSG was subject to a legislated oversight regime that required the NSW Police Commissioner to carry out an annual audit of its operations and the Commission to monitor and report on the effectiveness of this annual audit. Furthermore these annual audits were directed at specific aspects of the operation of the PSG:

- whether the PSG as a whole was adhering to its charter and effectively performing its role as provided in its charter
- whether the members of the PSG were adhering to its charter
- whether proper procedures existed and were being adhered to by the PSG in connection with the use and payment of informants, and
- whether proper procedures existed and were being adhered to by the PSG for the recording and use of intelligence gathered by the PSG.

In practice these annual audits were conducted by a unit within NSW Police known as the NSW Police Audit Group.

8.2 CURRENT OVERSIGHT OF THE CTCC

The Commission sought information about the current oversight of the operations of the CTCC through the interviews it conducted with key CTCC staff. After discussing the previous PSG oversight regime, key CTCC staff were asked ‘are there currently any such regular checks on the operations, policies and procedures of the CTCC by another area of NSW Police such as the Audit Group?’.

The staff who were interviewed said that the CTCC was subject to the same oversight mechanisms as other NSW Police commands. They said that, like other commands, the CTCC was available for auditing by the Audit Group. One of the officers who was interviewed, expressed the view that special oversight was no longer needed if other commands such as the State Crime Command were not also required to have any special oversight provisions.

8.3 PERCEPTIONS OF BENEFITS AND DISADVANTAGES OF THE OVERSIGHT REGIME USED FOR THE PSG

In its interviews with key CTCC officers, the Commission incorporated questions to collect those officers' views on the benefits and/or disadvantages of different aspects of the oversight regime that had been used for the former PSG. The Commission did this so that if it were determined that some future oversight or monitoring scheme was required then attempts could be made to avoid what may have been considered less useful elements of the previous system and incorporate what may have been considered to be more useful elements.

The Commission also sought this information to ascertain these officers' attitudes to oversight from beyond the command more generally.

ANNUAL AUDIT BY NSW POLICE AUDIT GROUP

In the structured interviews, Commission staff outlined the audit requirements provided under Part 3 of the *Police Act 1990* and then asked each of the officers what they considered to be the benefits of such an audit as well as what they considered to be the disadvantages of such an audit. From the comments made, it is clear that some of the officers answered in terms of their views of the benefits/disadvantages of the annual audit of the PSG, while other officers expressed their views of the potential benefits/disadvantages that such an annual audit would have for the CTCC.

In summary, the benefits of the annual audit by the NSW Police Audit Group that were identified by these officers included:

- providing assurance on an annual basis that the systems, procedures and protocols are being adhered to and to ensure that the PSG did not go back down the path of the Special Branch
- enhancing the reputation of the Command, and
- providing feedback on areas that could be improved.

These officers considered that the following were disadvantages of the annual audit:

- it is a waste of time and resources both because of the amount of time taken by audit activities and because it duplicates the existing internal audits conducted by the command
- the frequency of the audit is disruptive, with the amount of time it takes
- it focuses on areas that do not require oversight by examining areas that are not areas of apparent risk
- it has a negative effect on the morale of officers as it is seen by some officers as a perceived lack of trust in their performance of their duties.

One officer said that, in his view, an annual audit is ineffective since it is analogous to 'closing the door after the horse has bolted'. He suggested that it was better to have

preventative strategies in place than attempting to detect past misconduct through an audit.

OVERSIGHT BY AN EXTERNAL AGENCY SUCH AS THE COMMISSION

In the structured interviews, after outlining that the Commission was required each year to review the audit conducted by NSW Police of the operations, policies and procedures of the PSG, each of the officers was asked what they considered to be the benefits of such oversight by an external agency and what they considered to be the disadvantages of such oversight. The perceived benefits and disadvantages of oversight by an external agency reported by these officers were similar to what they had considered to be the advantages and disadvantages of the annual audit by the NSW Police Audit Group.

In summary, the benefits of oversight by an external agency identified by these officers included their beliefs that this external oversight:

- enhances the reputation of the command with those in government and the community having confidence in what the command was doing
- provides an assurance to Government and the Parliament that the command is not falling back into the problems of the past
- brings a measure of independence and provides an independent perspective on what could be improved
- adds to the rigour of the process.

The disadvantages of oversight by an external agency that these officers identified included their concerns that such external oversight:

- draws an unnecessary distinction between the CTCC and other commands (these officers suggested that the CTCC is not different from other commands, terrorism is a crime like other crimes and the command has to gather evidence and subject it to the courts like other commands)
- has a negative effect on the morale of officers with the perception that those working in this area cannot be trusted
- may pose operational difficulties with law enforcement partners (such as the AFP and ASIO) if the information is provided to a third agency (that is, an external oversight agency). Agencies that supply information to the CTCC may not want it reviewed by a third, external agency.

One officer said that he thought that there would only be a disadvantage in having oversight by an external agency if the oversight were done without an understanding of police practice, that is, if it were done by someone who does not understand what the PSG (or CTCC) is doing and why it is being done.

It should be noted that some of those interviewed said that they did not see any disadvantages of external oversight in relation to the activities of the PSG.

8.4 SUGGESTIONS FOR NATURE OF OVERSIGHT REQUIRED BY THE CTCC

Those who were interviewed were asked 'what, if any, external monitoring or oversight arrangements do you think are required to adequately manage the misconduct risks that may be faced by officers working in the CTCC?'.

The majority of those interviewed suggested that they did not think that any separate oversight was required. Instead, they suggested that the oversight of the CTCC should be the same as the oversight currently required of other specialist commands in NSW Police (that is, the CTCC should be the subject of audit, but in keeping with the NSW Police framework of auditing, such an audit should only occur once every three years). They based their views on the following arguments:

- the functions of the CTCC are the same as functions of other NSW Police commands
- where the CTCC has special powers – e.g. Terrorism Police Powers, Covert Search Warrants, Preventative Detention – NSW Police has worked with the Attorney General's Department to produce appropriate oversight mechanisms, and
- the command has changed since Special Branch, for example, the Dignitary Protection Unit does not do investigations because of the previous problems with Special Branch.

Other officers suggested that any oversight requirements that are introduced need to be very targeted. One officer, who said he thought that there should be some external oversight, said that it would be desirable to do a risk assessment and target only those areas that require special oversight. This officer suggested that 'carte blanche' oversight is not useful. He further suggested that some of the new policing powers may need oversight until appropriate procedures are in place.

A second officer suggested that he did not think that oversight of the CTCC would be necessary so far as the functions pertaining to the investigation of terrorism were concerned. However, he suggested that as the work starts moving into the area of politically motivated violence, there may be things that need to be done differently. This officer said that he thought that it was important to realise the sensitivity of public order management and the right to protest legally. He suggested that it might be appropriate to confine the oversight to information gathering, recording and intelligence management in the area of public order management only. This officer suggested that the reason for monitoring this area of work was a result of the difficulty in delineating between people involved in legitimate protest versus those involved in politically motivated violence.

One of the unit leaders suggested that it was important to consider the threshold question of 'would this area require special auditing/oversight arrangements, if it were part of a different command?'.

8.5 OVERSIGHT OF OTHER NSW POLICE COMMANDS

Given that the CTCC is currently subject to the same oversight provisions as other NSW Police commands, the Commission sought to understand the nature of that oversight.

SELF-ASSESSMENT USING THE CMF

As discussed in Chapter 5, commands are encouraged to conduct self-assessment audits using the CMF.

The material supplied to the Commission by NSW Police concerning the CMF indicated that NSW Police was moving towards self-assessments by individual commands and moving away from audits conducted by the Audit Group:

> Self-assessment is now considered best practice throughout the private sector, providing a balance between reporting needs and unnecessary external scrutiny. …
>
> The external, sometimes punitive audits of the past will generally no longer be imposed on local commands (NSW Police intranet, downloaded by NSW Police 30 March 2006, provided to the Commission 26 April 2006).

ORGANISATIONAL REVIEW AND SUPPORT

The NSW Police Audit Group, which previously conducted annual audits of the PSG, no longer exists in the same form. Following an organisational restructure within NSW Police in October 2005, the former Audit Group became part of a new 'Commissioner's Inspectorate'. Subsequently 'Organisational Review and Support', which integrates the former functions undertaken by the Audit Group, Operations & Crime Review Team, Operational Readiness Audit, Executive Support Group, and Crime Management Faculty was established.

The NSW Police intranet describes the functions of Operational Review and Support as:

- to contribute to good corporate governance by undertaking command, thematic, strategic, and project performance reviews including the Operations & Crime Review (OCR) process
- to improve organisational performance by identifying corporate risks and recommending appropriate treatment options
- to provide support to operational, specialist and corporate commands (i.e. crime management, behavioural science, investigations, intelligence, business planning etc).

The description of Organisational Review and Support provided on the intranet continues as follows:

> Organisational Review & Support aims to provide a comprehensive overview of a Command's operational capability. By combining the functions of the former Audit Group, Crime Management Faculty and Executive Support Group, Local Area and Region Commanders will be given a more holistic evaluation of Command performance. The evaluation will then proceed to a new revamped OCR process where the bigger issues impacting upon Commands and the organisation as a whole may be discussed at a strategic level. It is envisaged that these discussions during the OCR will form the nucleus of the Support Package that will be provided by the Commissioner's Inspectorate, in close consultation with both [local area command] and Region (downloaded from the NSW Police intranet on 12 July 2006).

Organisational Review and Support is in the process of establishing its procedures. The Commission has been informed that the former Audit Group used to try to look at every command in the state at least once every three years. The Commission understands that at the time of drafting this report (July 2006), Organisational Review and Support does not currently have a regime to ensure that all commands will be subject to an audit conducted by personnel from outside that command. Hence the regularity with which any command would be audited by personnel from outside the command is currently not clear. It is possible that the CTCC would at no time be subject to audit by the Commissioner's Inspectorate.

8.6 OBSERVATIONS

Unlike the former PSG, which was subject to a legislated oversight regime requiring an annual audit conducted by the NSW Police Audit Group and monitoring of that audit by the Commission, much of the oversight of the CTCC is currently based on supervision and self-assessment. While the Commission values the importance of self-assessment, it considers that oversight also plays a useful role in deterring future misconduct.

Key CTCC officers perceived that the benefits of an annual audit and oversight by an external agency were that such measures provide an assurance to Government and the Parliament and can enhance the reputation of the command. However, some also commented that the audit conducted on the PSG was a waste of resources as it duplicated internal checking processes, was time consuming and focused too broadly including areas that were not at risk. Some officers also considered that these audits had an adverse effect on morale through a perceived lack of trust.

The Commission is of the view that for any oversight planned, care should be taken to design the oversight to carefully target what is being monitored and minimise the resources required and the potential disruption caused. It is arguable that the audit methodology applied to the PSG canvassed the potential for misconduct too widely rather than specifically focussing on the misconduct risks faced by the PSG that were different from the misconduct risks faced by other NSW Police commands, which had originally been a concern in the Special Branch. In terms of morale, it is important to present clear messages that any oversight is a result of the nature of specific functions carried out, it is not the result of any specific concerns about the officers who are employed in the area.

When asked for their suggestions concerning the types of monitoring arrangements necessary to adequately manage the misconduct risks that may be faced by officers working in the CTCC, the majority of officers interviewed said that they thought that

the oversight for the CTCC should be the same as the oversight arrangements for other NSW Police commands. They tended to argue this on an equity basis, that is, that the CTCC should be treated in the same way as other commands. The Commission does not accept the argument that oversight should be based on equity considerations. Instead the Commission is of the view that the need for oversight should be determined by the nature of the risk. This was the case for the oversight of the PSG which was recognised as being under much greater scrutiny than any other NSW Police command. In particular the Commission considers the need for any oversight or special monitoring of the CTCC should be based on considerations such as whether the misconduct risks faced by the CTCC differ from those faced by other commands and the nature of the mechanisms that are in place to address any CTCC misconduct risks that are different from those faced by other commands. These, and related issues, are considered in Chapter 9.

The Commission supports the view expressed by some officers that any oversight should be targeted to those areas which are associated with a special risk. It is of interest to note that one officer suggested that it might be appropriate to confine the oversight to information gathering, recording and intelligence management in the area of public order management because of the difficulty in delineating between people involved in legitimate protest versus those involved in politically motivated violence.

8.7 SUMMARY OF KEY POINTS

1. Unlike the former PSG, the CTCC is not the subject of any special oversight requirements. Like other commands, the CTCC is encouraged to conduct self-assessment audits using the CMF.
2. The former PSG oversight regime is seen by key CTCC staff as having the advantages of providing an assurance to Government and the community that the PSG did not go back down the path of Special Branch, as well as providing feedback on areas of its operation that could be improved. However, it is also seen as having disadvantages, including being a waste of time and resources, being disruptive, being focused too broadly including areas that were not at risk and having a negative effect on the morale of officers. Operational difficulties of law enforcement partners not wanting the information they provide to the CTCC being reviewed by an external agency was raised as a further disadvantage of oversight by an external body.
3. The majority of the key CTCC staff who were interviewed suggested that they did not think that any separate oversight was required to adequately manage the misconduct risks that might be faced by officers working in the CTCC. Others suggested that any oversight requirements that are introduced need to be very targeted.
4. The NSW Police Audit Group which previously conducted annual audits of the PSG no longer exists. A new unit, Organisational Review and Support, which integrates a number of review functions in addition to the functions of the former Audit Group, has been established.
5. The regularity with which any command would be audited by personnel from outside the command is currently unclear.

9. ASSESSMENT

The Commission undertook this assessment of the CTCC's management of misconduct risks to provide a more informed basis on which to consider whether the CTCC requires oversight that is any different from that considered necessary for other NSW Police commands. This chapter begins with a discussion of what the Commission has learnt in relation to four issues relevant to the decision of what, if any, special oversight or monitoring arrangements are needed to adequately manage the misconduct risks that may face officers working in the CTCC (see Section 9.1). From the information that was collected and analysed for this assessment, several areas in which the CTCC could further strengthen its capacity to resist misconduct became apparent. These are discussed in Section 9.2. The chapter concludes with a statement of the Commission's position concerning appropriate oversight (see Section 9.3).

In considering this assessment it is important to realise that the Commission restricted its collection of information to units under the supervision of the Assistant Commissioner Counter Terrorism and Public Order Management. The Commission has neither any basis for nor any intention to suggest that the performance of the CTCC is any better or poorer than any other command in NSW Police in terms of misconduct risk management.

9.1 RELEVANT CONSIDERATIONS

From the outset, it should be noted that the Commission's interest in the misconduct risks of the CTCC has stemmed from the CTCC's historical connections with the former Special Branch and the weaknesses identified with the operations of the former Special Branch. The Commission has no reason to believe that individual officers who are appointed to work in the CTCC are more likely to engage in misconduct than individual officers who work in other NSW Police commands. The Commission's focus in this assessment is on the nature of the work undertaken by the CTCC and on the management of any misconduct risks associated with this work, rather than on the conduct of individual officers.

In determining whether or not the CTCC requires a different oversight regime from other NSW Police commands, four issues warrant consideration:

- Do the misconduct risks faced by the CTCC differ from those faced by other commands?
- What mechanisms are in place to minimise any CTCC misconduct risks that are different from those faced by other commands?
- What lessons have been learnt from the investigations into the former Special Branch?
- What features of oversight are desirable and what oversight is currently provided?

These issues are considered, in turn, below.

DO THE MISCONDUCT RISKS FACED BY THE CTCC DIFFER FROM THOSE FACED BY OTHER COMMANDS?

Three questions are of interest:

- Do the functions of the CTCC include functions associated with the documented problems of the former Special Branch and the functions of the PSG that were seen to require special monitoring?
- Are there additional aspects of the CTCC's work which may be associated with misconduct risks not commonly faced by other commands?
- In what ways do the misconduct risks facing the CTCC differ from the misconduct risks facing other NSW Police commands?

Each of these questions is discussed separately below.

Do the functions of the CTCC include those undertaken by the former Special Branch and by the former PSG?

Notwithstanding the name of the command, the work undertaken by the CTCC is broader than counter-terrorism policing. In addition to collecting information in relation to acts of terrorism and other politically motivated violence, the Intelligence Unit of the CTCC collects information to assist in dignitary protection and information to support the Public Order Riot Squad.

The CTCC, like the former PSG and the former Special Branch before it, provides close personal protection for dignitaries, carries out related intelligence gathering and threat assessments, and is responsible for tactical and operational analysis, intelligence gathering and liaison with other relevant agencies, in relation to those who present a risk of politically motivated violence including terrorist activity.

While the CTCC's work may be broader than that of the former PSG, it incorporates all of the functions of the former PSG and the former Special Branch. This includes the functions that were associated with the documented problems of the former Special Branch and the functions of the PSG that were seen to require special monitoring.

Are there additional aspects of the CTCC's work which may be associated with misconduct risks that are uncommon in other commands?

The Commission understands that the functions of the CTCC are broader than those of the former PSG and the former Special Branch. The CTCC has a specific responsibility for critical infrastructure protection, a larger investigative capacity and, more generally, significantly more resources than the units that have preceded it. The Commission has no reason to consider these differences in size and function as being likely to be associated with misconduct risks that would be different either from those that faced officers who worked in the former PSG or those facing officers working in other NSW Police commands.

The Commission also considered whether the misconduct risks that the CTCC nominated were indicative either of functions over and above those carried out by the former Special Branch or by the former PSG, or were indicative of any additional aspects of the CTCC's work that may be associated with misconduct risks that are uncommon in other commands. In its written response to one of the questions posed by the Commission, the CTCC identified the following as the list of potential misconduct risks faced by officers working in the command:

- Unauthorised release or misuse of information – either deliberately or accidentally – especially information from third parties
- Inappropriate storage of information
- Inappropriate collection of information
- Recruitment of officers for information by external agencies (national security issue)
- Improper associations
- Misuse of motor vehicles
- Misuse of mobile phones
- False overtime claims
- Misuse of covert licences.

It is possible that some of these misconduct risks, because of the nature of the work of the CTCC, may be either more likely to occur or have greater consequences if they were to occur in the CTCC than if they were to occur in other commands. For example, because of the nature of the information it collects and manages, the following misconduct risks may have greater consequences if they were to occur in the CTCC than if they were to occur in some other commands: 'recruitment of officers for information by external agencies', 'inappropriate storage of information' or 'inappropriate collection of information'. Similarly, because of its responsibility for dignitary protection, 'improper associations' may be more of a risk for the CTCC than it is for some other commands. However, these risks do not arise from new functions of the CTCC. They arise from the same functions that were carried out by the former Special Branch and the former PSG. Hence such misconduct risks would not be additional to those faced by officers who worked in the former Special Branch or the former PSG. Also misconduct risks concerning the unauthorised release of information and inappropriate associations are risks faced by officers working in many NSW Police commands.

Similarly, other nominated risk areas (such as 'misuse of motor vehicles', 'misuse of mobile phones', and 'false overtime claims') which, based on advice from the command may perhaps be greater than for some other commands, would not be specific to the CTCC and do not arise from any new or different functions from those carried out by the former PSG or the former Special Branch.

In relation to the legislative changes in counter-terrorism policing, it is important to note that the counter-terrorism police powers are not confined to officers employed in the CTCC. With the exception of the powers concerning covert search warrants, the other police powers provided in the *Terrorism (Police Powers) Act 2002* can be employed by any NSW Police officer, though the use of these powers can be

authorised by only a relatively small number of individuals and can only be authorised under quite specific circumstances. To the extent that these powers provide additional misconduct risks, such misconduct risks would not be confined to officers working within the CTCC.

The only power that may be exercised by CTCC staff that is additional to either those exercised by former PSG staff or those exercised by any NSW Police officer, is the ability for 'eligible officers'[30] to enter, without any occupiers' knowledge, and search premises under the authority of a special covert search warrant (Section 27O of the *Terrorism (Police Powers) Act 2002)*. Hence the Commission would consider that the ability, under certain restricted circumstances, to execute a covert search warrant is the only additional aspect of the CTCC's work which may potentially be associated with misconduct risks that are different from those faced by officers working in other commands.

In what ways do the misconduct risks faced by the CTCC differ from the misconduct risks faced by those working in other commands?

The Commission recognises that many components of the CTCC's functions are similar to functions carried out by other commands. For example, as some of the interviewed CTCC officers identified, some investigations carried out by the CTCC may not be dissimilar from investigations carried out by the other areas of NSW Police such as those conducted by the investigative squads of the State Crime Command. However, while there are some similarities between the functions of the CTCC and some other commands, the Commission considers that there are also points of difference. The Commission is of the view that these differences primarily concern the nature of the information collected by the CTCC.

While it is accepted that a number of commands in NSW Police may be involved in activities and initiatives to prevent crime, the Commission considers that crime prevention represents the predominant aspect of the CTCC's work. From the Commission's observations, most of the activities of the CTCC are directed towards the prevention of politically motivated violence (including terrorism) and the protection of dignitaries. This predominant focus on prevention establishes a major point of differentiation between the CTCC and most other commands in NSW Police.

This focus on prevention necessitates that, as part of the legitimate work of the CTCC, information will be collected on some individuals who will not be involved in subsequent acts of violence. For example, in order to properly assess risk, to afford appropriate protection and prevent harm to dignitaries, it is likely that information and intelligence will need to be collected on the dignitaries themselves and on those associated with them. In addition, to properly advise in respect of threats to public order, information and intelligence is also likely to be collected on those engaged in legitimate protest but who may present a risk, perhaps through association with those suspected of engaging in politically motivated violence, of engaging in violence in certain circumstances.

While the collection of information to prevent politically motivated violence (including terrorism) and to assist in dignitary protection is a fundamental aspect of the CTCC's functions, such a role has in the past been associated with misconduct. This was the

[30] Officers employed in a NSW Police group designated as the 'terrorism investigation group' by the Commissioner of Police or an eligible member of the Crime Commission.

case when the former Special Branch was found to be gathering information and maintaining files on people who posed no threat of politically motivated violence.

WHAT MECHANISMS ARE IN PLACE TO MINIMISE ANY CTCC MISCONDUCT RISKS THAT ARE DIFFERENT FROM THOSE FACED BY OTHER COMMANDS?

In this section the Commission firstly considers the mechanisms that the CTCC has put in place to minimise the problems previously identified in the practices of the former Special Branch. Secondly it considers the mechanisms that are in place to address other misconduct risks, not common in other commands, that are associated with other functions or powers (i.e., the execution of covert search warrants) exercised by the CTCC.

What mechanisms are in place to minimise the problems previously identified in the operations of the Special Branch?

It has been ten years since the Royal Commission. During that period NSW Police has undergone many changes.

As outlined in Chapter 2 of this report, the former Special Branch was identified as having major weaknesses in the areas of:

- disregard for its charter and a lack of accountability
- information gathering on people who posed no threat of politically motivated violence or similar matters (inappropriate targeting) and the belief that it could be used for political advantage against persons on whom 'dirt files' had been kept
- an unacceptable overlap between the functions of information gathering and protection of VIPs, leading to information being held about VIPs and public figures, rather than those who posed a threat to them
- informant management and the payment of informants
- poor record keeping practices
- ineffective and outdated intelligence system
- poor supervision, and
- unsatisfactory recruitment practices.

Since the time that these criticisms were made of the operations of the Special Branch, NSW Police has revised or developed policies and systems in some of these areas. Unlike the former Special Branch, the CTCC does not rely on stand-alone systems. Instead it uses NSW Police corporate systems for information management, informant (or source) management, and for recruitment. Some of these corporate systems include facilities which enable regular audits to be conducted.

While the use of corporate systems does not guarantee that some CTCC staff will not engage in misconduct at some time, it does mean that the systems used by the

CTCC are as accountable and as transparent as the systems used by other NSW Police commands.

On the premise that the use of informants by CTCC officers is not intrinsically different from the use of informants by other areas of investigative policing, the CTCC's use of the NSW Police corporate source management policy provides some assurance that the CTCC's misconduct risks are no greater than those of other commands in relation to informant management and the payment of informants. Similarly, the CTCC's use of corporate information management and recruitment systems provides some assurance that the CTCC's misconduct risks are no greater than other commands in relation to the following of the criticisms made of the former Special Branch:

- record keeping practices
- reliance on an ineffective and outdated intelligence system, or
- unsatisfactory recruitment practices.

While supervision was identified as a weakness in the operation of the former Special Branch, the importance of good supervision and leadership is not unique to the CTCC. The Commission has no reason to consider that the quality of supervision within the CTCC is an area of greater misconduct risk than supervision within any other command.

On the other hand, the Commission is of the view that, simply as a reflection of the functions the CTCC carries out, the following areas, previously identified as problems in relation to the former Special Branch, remain as a greater potential risk within the CTCC than within other commands:

- information gathering on people who posed no threat of politically motivated violence or similar matters (inappropriate targeting) and the belief that it could be used for political advantage against persons on whom 'dirt files' had been kept
- an overlap between the functions of information gathering and protection of VIPs, leading to information being held about VIPs and public figures, rather than those who posed a threat to them.

These problem areas are closely related to the 'potential for disregard for its charter and accountability' which was also mentioned in relation to the operations of the former Special Branch.

What mechanisms are in place to address misconduct risks, not common in other commands, associated with other functions or powers of the CTCC?

As discussed earlier, when the Commission sought to identify whether the CTCC has additional functions or powers that may be associated with misconduct risks that are different from those faced by officers working in other commands, the Commission saw such additional aspects of the CTCC's work as being confined to the ability to execute a covert search warrant under certain restricted circumstances. When introducing the legislation that enabled covert search warrants by amending the *Terrorism (Police Powers) Act 2002* – the *Terrorism Legislation Amendment*

(Warrants) Act 2005 – the need for safeguards and accountability mechanisms was recognised. Mr Bob Debus, the Attorney General and Minister for the Environment, described the powers as 'extraordinary' and said that these powers 'would only be permitted with the strictest of safeguards' (NSW Legislative Assembly 2005, p. 16940). The accountability requirements that were introduced as part of this legislation include:

- the eligible judge must cause a record to be made of all relevant particulars of the grounds that he or she has used to justify or refuse the issue of the warrant (section 27L)
- a person to whom a covert search warrant was issued must report back to the judge who issued the warrant about the execution of the warrant within 10 days after it was issued or after it expired (section 27S)
- annual reports must be made to the Attorney General and the Minister for Police regarding the exercise of these powers (section 27ZB), and
- the scheme is subject to independent monitoring by the NSW Ombudsman for a period of two years (section 27ZC).

Given that these provisions commenced in September 2005, the report outlining the results of the independent monitoring being conducted by the NSW Ombudsman will not be available before late 2007.

Furthermore, the legislation states that an application for such a warrant can only be sought in the following (limited) conditions:

- that a terrorist act has been, is being or is likely to be committed, and
- that the entry to and search of premises will substantially assist in responding to or preventing the terrorist act, and
- that it is necessary for the entry and search of those premises to be conducted without the knowledge of any occupier of the premises (section 27C).

WHAT LESSONS HAVE BEEN LEARNT FROM THE INVESTIGATIONS INTO THE FORMER SPECIAL BRANCH?

Soon after the investigations occurred, the lessons – as reflected in the actions taken – appear to have been clear. The former Special Branch was disbanded. The former Commissioner of Police, the Royal Commission and the NSW Government each identified the need for a range of safeguards as well as the need for a special oversight regime to be established for any unit that was to replace the Special Branch. As a result an oversight regime, formalised in legislation, was established for the PSG. This oversight regime involved annual audits directed at specific aspects of the operation of the PSG and the monitoring of these audits by the Commission.

With the passing of time, the broad lesson that the nature of the work carried out by the former Special Branch (subsequently carried out by the former PSG and now carried out by the CTCC) is associated with particular risks appears to have been lost. When the Commission asked NSW Police whether the CTCC is recognised as

a command for which special misconduct risks exist due to its functions, NSW Police responded that 'it was unaware of any identified special misconduct risks derived from the CTCC's functions'. It added that 'individual commands, including the CTCC, are encouraged by the CMF process to develop local input and processes relevant to their environment'. It was clear from its response that NSW Police considered the CTCC to be a command like any other. That is to say, it was clear that NSW Police had not identified the CTCC to have special risks as a direct consequence of the CTCC assuming the role previously undertaken by the Special Branch, notwithstanding the problems which had been documented in relation to the practices of the former Special Branch.

The Commission has also noted that officers who join the CTCC are not provided with information concerning the investigations into the former Special Branch and how the weaknesses identified in the way the former Special Branch discharged its functions might highlight pitfalls to be avoided by those working in the CTCC. Currently there do not seem to be any reminders in place to prompt individual officers, the command or the organisation as a whole to use the lessons from the documented weaknesses of the former Special Branch as a means of strengthening current practices.

WHAT FEATURES OF OVERSIGHT ARE DESIRABLE AND WHAT OVERSIGHT IS CURRENTLY PROVIDED?

Desirable features of oversight

The Commission considers that oversight has a preventative role. Identifying that some particular area of work is to be oversighted from outside the command or actively supervised from within the command tends to focus attention on that area of work and, as a result, deter future misconduct in that area. However, in designing appropriate oversight measures, the Commission is also of the view that care should be taken to ensure that the ownership and responsibility for the work remains with those who undertake the work.

The Commission is of the opinion that the extent and type of oversight should be tailored to the nature of the risk to be managed and care should be taken in its design so that it is useful and so that any monitoring activities are not unnecessarily disruptive or resource intensive. This was not the case with the audits conducted on the operations, policies and procedures of the former PSG. These audits were criticised by some key CTCC officers as focussing on areas that were not at risk and duplicating internal checking processes. While the primary purpose of oversight is to deter future misconduct, the oversight must be designed in such a way that it is appropriately focussed and that it would be able to detect inappropriate conduct if it were to occur.

Furthermore, the Commission recognises that legislating the type of oversight and the frequency with which it is to occur in connection with one functional area of NSW Police is restricting for both NSW Police and any external oversight agency involved, providing little flexibility as to the roles played by each agency and the frequency of the audits.

Moreover, the Commission recognises that the work and structure of the CTCC are subject to change. The misconduct risks associated with functions performed by the

CTCC and the naming of the functional unit (or units) within NSW Police that undertakes these functions may be subject to change over time. For these reasons, it is desirable for any oversight or monitoring arrangements to be linked to the functions performed, rather than to the name of the unit that currently performs those functions and be sufficiently flexible to allow for changes in misconduct risks that result from changes in the functions performed.

Oversight currently provided

Much of the oversight of the work of the CTCC, like the oversight of the work of other NSW Police commands, is currently based on supervision and self-assessment audits from within the command. To the Commission's knowledge, there are currently no plans by NSW Police to monitor the work of the CTCC any differently from the way it monitors the work of other commands. That is to say, there are currently no plans for NSW Police staff from beyond the command to audit aspects of the CTCC's work.

Unlike other commands, the CTCC's charter requires the establishment of the Counter Terrorist Management Committee (CTMC). This Committee, which is comprised of the Commissioner of the NSW Crime Commission, the NSW Police Deputy Commissioner responsible for the CTCC and the Director General of the Ministry, is responsible for 'oversighting the core responsibilities of the CTCC' as well as 'the CTCC's involvement in joint operations with other similar agencies' such as the NSW Crime Commission, ASIO and the AFP. The Commission has been informed that the CTMC is not involved in the day-to-day administration and control of the CTCC personnel. Instead the CTCC's administration and control, like other commands within NSW Police, is based on the CMF.

9.2 OPPORTUNITIES FOR STRENGTHENING RESISTANCE TO MISCONDUCT

In collecting and analysing information for this assessment, several opportunities for the CTCC to further strengthen its capacity to resist misconduct became apparent. Any weaknesses in current practices that are described in this section are provided as a means of identifying opportunities for improvements. They do not, of themselves, contribute to an argument that the CTCC requires an oversight regime which is different from the oversight regime required of the work of other commands.

STRENGTHS

Prior to describing the opportunities for improvements, some of the strengths of the CTCC's current practices are outlined to provide a context in which to consider the areas for improvement. Firstly, unlike the former Special Branch, the CTCC uses NSW Police corporate systems rather than stand-alone systems.

Also from the interviews that Commission staff conducted with key CTCC officers, it was clear that these senior CTCC officers had given thought to the types of misconduct risks likely to be faced by officers working in the CTCC and to different strategies for responding to these risks. These officers also impressed as being open to discussion on these issues.

The minutes of the CTCC's CMT meetings illustrate clear examples of where the CTCC's CMT has looked beyond the conduct of the individual officer to identify the wider implications of individual complaints. These minutes also provide examples of where this CMT has taken action to tackle the issues underlying some of these complaints.

OPPORTUNITIES

The main areas in which the Commission considers that the CTCC can strengthen its capacity to resist misconduct are:

- preparing and implementing a documented misconduct risk management plan, and
- equipping its officers for the misconduct risks that they may encounter in their work.

Preparing and implementing a documented misconduct risk management plan

The Commission is of the view that all commands should have effective and documented processes in place for identifying, assessing and responding to potential misconduct risks. Such a documented misconduct risk management plan could be part of a broader risk management plan or it could take the form of a separate corruption resistance plan.

The absence of documentation in the case of the CTCC means that it is difficult to understand how cohesive or comprehensive its current misconduct risk management processes are. While the Commission has been informed that the CTCC's CMF is tailored for the requirements of this particular command, it is not clear that this is the case. For example, the misconduct risks that the CTCC provided in response to the information sought for this assessment and the actions or processes to manage these risks, are not specifically included in the CTCC's CMF.

At the time this exercise was conducted, the CTCC lacked documentation of the individual misconduct risks faced by CTCC officers. As a consequence it lacked documentation that linked the treatment strategies to specific misconduct risks. In the material it provided to the Commission, the CTCC did not identify the range of options for treating risks or provide any assessment of the advantages and disadvantages of different treatment strategies. From the information provided, it is not clear whether the CTCC has strategies in place for each of the misconduct risks its officers may encounter. The lack of documentation casts doubt upon the comprehensiveness of the CTCC's misconduct risk management process.

In order to improve its capacity to resist misconduct, the Commission suggests that the CTCC (and all other commands) should document, and where necessary further develop, its misconduct risk management strategy, including documenting:

- the strategies it uses to identify its misconduct risks
- a list of the misconduct risks it has identified using these strategies

- for each misconduct risk, an assessment of the likelihood of this risk occurring, its consequences if it were to occur and an overall rating of the assessed seriousness of the risk of this area of misconduct
- for each misconduct risk, the range of options for treating the risk and an assessment of the advantages and disadvantages of the different treatment strategies
- for each misconduct risk, the strategies that the command has decided to use in response to that risk, and
- a timeframe when the risks, assessments of the seriousness of the risks and treatment strategies will next be reviewed and a process for that review.

In the case of the CTCC, the misconduct risk management plan should use the CTCC's charter as its foundation. Additional opportunities exist for better integrating the material in the CTCC's charter with the CTCC's CMF and with its induction and training materials.

In addition to preparing a documented misconduct risk management plan, it is necessary to ensure that the plan is implemented and regularly reviewed.

Equipping officers for the misconduct risks they may face through their work in the CTCC

A second area for strengthening the command's ability to resist misconduct would be by providing CTCC officers with information about the specific misconduct risks that are associated with their work in the CTCC and how best to respond to these misconduct risks. Some steps that the CTCC could consider in this regard include:

- informing CTCC officers of the specific misconduct risks they might encounter in their work and how these officers should respond if they find themselves in such circumstances
- providing information to CTCC officers about the investigations into the former Special Branch and how the weaknesses identified in the way the former Special Branch discharged its functions can highlight pitfalls to be avoided by those working in the CTCC
- making explicit reference in induction material and other training material to the CTCC's charter and the associated limits to the range of intelligence and investigations that the CTCC should undertake and what this means in practice.

More generally it is important for individual officers, the command, and the organisation as a whole to recognise the value of the lessons from the documented weaknesses of the former Special Branch as a means of strengthening current practices.

While these opportunities would appear particularly important for the CTCC given the changing environment it faces, where they do not already have such a documented process in place other NSW Police commands may also benefit from preparing and implementing a documented misconduct risk management plan.

9.3 OVERSIGHT REQUIRED

The Commission considers that like officers from any command, the officers who work in the CTCC face a range of misconduct risks. While most of these misconduct risks are pertinent to officers working in other commands, some misconduct risks arising in the CTCC environment would be uncommon in other commands. It is to these misconduct risks, which are not common to NSW Police as a whole and which would be faced by any unit undertaking the same functions as the CTCC, that this assessment has been addressed.

A MORE TARGETED FORM OF MONITORING THAN THAT PREVIOUSLY REQUIRED FOR THE PSG

The Commission is of the view that, because of the nature of these uncommon risks, some aspects of the work of the CTCC warrant careful monitoring, but that such monitoring can be more tailored and should be more focused than in the past. The Commission considers that less aspects of the work of the CTCC require some form of special attention than was the case for the PSG because, unlike the former Special Branch which used stand-alone systems, the CTCC uses corporate systems for its storage of information, management and payment of informants, and recruitment.

Previously, Part 3 of the *Police Act 1990* required that the audit of the PSG specifically focussed on whether proper procedures existed and were being adhered to by the PSG in connection with the use and payment of informants. While the Commission recognises that informant management is a corruption risk for law enforcement agencies internationally, and hence presents a corruption risk for all investigative areas of NSW Police that use informants, the Commission is of the view that informant (or source) management does not pose a greater risk to the CTCC than it does to other areas of NSW Police. As such the Commission considers that informant management and the payment of informants by the CTCC should be subject to the same form of monitoring as that used for informant management undertaken by other commands.

The Commission is of the view that investigations to prevent acts of terrorism, while having different operational risks from other investigations, largely present the same misconduct risks as those faced by other areas of policing that conduct criminal investigations.

While the execution of covert search warrants is an area of CTCC operations that may require special monitoring in the future, the Commission is of the view that consideration of the need for any additional oversight in this area should be deferred until the findings of the NSW Ombudsman's report monitoring the first two years operation of this aspect of the legislation become available.

FOCUS ON APPROPRIATE TARGETING AND APPROPRIATE RETENTION (AND DISPOSAL) OF INFORMATION

The Commission sees that the misconduct risks that are different and which require special management are restricted to quite specific areas of the work undertaken by the CTCC. In particular, the Commission considers that the misconduct risks that

initially require some form of special management are those that pertain to the possibility of:

- inappropriate targeting, and
- maintaining files on those who are unlikely to pose a threat of politically motivated violence.

The nature of the information collected by the CTCC, like the information collected by the former Special Branch and the former PSG, may cause some people to fear the creation and maintenance of 'dirt files' on individuals, even if this fear is misplaced. While the Commission considers that such misconduct is unlikely, because its consequences would be large if it were to occur the Commission believes that these areas warrant careful monitoring. The purpose of such monitoring is to focus attention on these areas as a means of deterring potential misconduct and to provide an effective reminder of the lessons from the investigations into the operations of the former Special Branch.

THE WAY FORWARD

The Commission considers that the way forward should include an improved CTCC misconduct risk management process to enable the CTCC to improve its capacity to identify and respond to current and future misconduct risks, as well as specific monitoring of the practices and procedures used by the CTCC to manage targeting and information retention (and disposal). Specifically, the Commission is of the view that the following needs to occur:

1. The CTCC (at the command level) and NSW Police (at the corporate level) should document their recognition of the inherent misconduct risks for any unit that undertakes the work of the former Special Branch and document the lessons, for those currently undertaking this work, to be learnt from the investigations undertaken into the work of the former Special Branch
2. The CTCC to more generally strengthen its capacity to resist misconduct, as discussed in Section 9.2, by:
    - preparing and implementing a documented misconduct risk management plan
    - equipping its officers for the misconduct risks they may face through their work in the CTCC by informing them of the specific misconduct risks they might encounter in their work and how these officers should respond if they find themselves in such circumstances, and
3. NSW Police to impose some form of monitoring that directly focuses on minimising the potential for inappropriate targeting and retention of inappropriate information which may be perceived as 'dirt files'.

The Commission does not wish to prescribe the form of monitoring to be used by NSW Police. The Commission considers this as a management issue for NSW Police, but believes that clearly defined, transparent procedures need to be developed and promulgated. The Commission does not see that further oversight by an external agency needs to be mandated at this stage. The current absence of a

legislative provision for auditing and monitoring does not in any way preclude the Commission from exercising its functions and powers in connection with the CTCC. The Commission is able to intervene either in direct response to a complaint or when it has a reason to believe that it would be in the public interest to do so. Also the management of any complaints about CTCC officers remains subject to the oversight of the NSW Ombudsman's Office.

The Commission will retain an interest in this area until it is satisfied with the systems put in place by the CTCC and by NSW Police to manage these potential misconduct risks.

GLOSSARY

Command Management Framework	NSW Police self-assessment audit tool.
Key CTCC staff	one of the information collection strategies used in this assessment of misconduct risk management involved the Commission conducting structured interviews with what is termed 'key CTCC staff' throughout this report. These 'key CTCC staff' included: • both officers who held the position of Assistant Commissioner Counter Terrorism and Public Order Management during the period the Commission was collecting its information • the Commander of the CTCC • the team leaders or acting team leaders of the Dignitary Protection Unit, the Intelligence Unit, and the Investigations Unit, and • the Commander of the Public Order and Riot Squad (PORS).
Misconduct risk	an organisational vulnerability for an employee to engage in fraud, corruption or other forms of misconduct that arises from the nature of an employee's work.
Misconduct risk assessment	the application of risk management principles and techniques in the assessment of the risk of misconduct (cf. Standards Australia 2003, p. 11).
Politically motivated violence	acts or threats of violence or unlawful harm that are intended or likely to achieve a political objective, whether in Australia or elsewhere, including acts or threats carried on for the purpose of influencing policy or acts of a government, whether in Australia or elsewhere; or acts that involve violence or are intended or are likely to involve or lead to violence and are directed to overthrowing or destroying or assisting in the overthrow or destruction of the government or the constitutional system of government of the Commonwealth or of a State or a Territory; or acts that are terrorism offences; or acts that are punishable by specified sections of the Crimes *(Foreign Incursions and Recruitment) Act 1978*, *Crimes (Hostages Act) 1989*, *Crimes (Ships and Fixed Platforms) Act 1992*, *Crimes (Aviation) Act 1991*, *Crimes (Internationally Protected Persons) Act 1976* ; or threaten or endanger any person or class of persons specified by the Minister for the purposes of this subparagraph by notice in

	writing given to the Director-General (*Australian Security Intelligence Organisation Act 1979*, s. 4).
Politically motivated Violence (cont'd)	for the purpose of this assessment, the Commission has included acts of terrorism within the definition of politically motivated violence.
Protective Security Coordination Centre (PSCC)	is a division of the Australian Government Attorney-General's Department, which coordinates protective security and counter terrorism arrangements between Australian Government, State and Territory agencies. As a member of the [National Crisis Committee], the PSCC channels communications between the Australian Government and States and Territories, including during a terrorist incident. During a terrorist incident the PSCC will provide authoritative reports to jurisdictions in the form of situation reports (National Counter-Terrorism Committee 2005, p. 2.4).
Protective Security Group	a unit of NSW Police that was established in August 1998 and absorbed into the Counter Terrorist Coordination Command in March 2003. Its mission involved the protection of dignitaries as well as analysis, intelligence gathering and liaison in relation to politically motivated violence or terrorist activity. (NSW Police (undated), p. 1).
Risk	the chance of something happening that will have an impact on objectives. A risk is often specified in terms of an event or circumstance and the consequences that may flow from it. Risk is measured in terms of a combination of the consequences of an event and their likelihood. Risk may have a positive or negative impact (Standards Australia & Standards New Zealand 2004, p. 4).
Risk analysis	systematic process to understand the nature of and to deduce the level of risk (Standards Australia & Standards New Zealand 2004, p. 4).
Risk assessment	the overall process of risk identification, risk analysis and risk evaluation (Standards Australia & Standards New Zealand 2004, p. 4).
Risk identification	the process of determining what, where, when, why and how something could happen (Standards Australia & Standards New Zealand 2004, p. 4).
Risk management	the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects (Standards Australia & Standards New Zealand 2004, p. 4).

Risk management framework	set of elements of an organization's management system concerned with managing risk (Standards Australia & Standards New Zealand 2004, p. 5).
Risk management plan	a document containing the: strategic context and objectives for risk management; analysis, assessment and prioritising of identified risks; and approach to manage risks (Public Accounts Committee 2005, p. xii).
Risk management process	the systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context identifying, analysing, evaluating , treating, monitoring and reviewing risk (Standards Australia & Standards New Zealand 2004, p. 5).
Risk reduction	actions taken to lessen the likelihood, negative consequences or both, associated with a risk (Standards Australia & Standards New Zealand 2004, p. 5).
Risk treatment	process of selection and implementation of measures to modify risk (Standards Australia & Standards New Zealand 2004, p. 5).
Special Branch	a unit of NSW Police that operated from 1948 until March 1997. It sought to provide relevant, current and specialised strategic and tactical intelligence concerning politically motivated violence and/or civil disorder, terrorist and extremist activity; and to plan and implement security procedures to ensure the safety of VIPs and property (Police Integrity Commission 1998, p. 10). It was disbanded by the Commissioner of Police following evidence put before the Royal Commission concerning abuses of power and lack of accountability.
Terrorism	those acts intended to intimidate the Government or the public involving serious injury or danger to people. Serious damage to property, or serious interference with an electronic system (NSW Legislative Assembly Hansard, 19 November 2002)
Terrorist Act	a 'terrorist act' is defined under Australian law as an act or threat, intended to advance a political, ideological or religious cause by coercing or intimidating an Australian or foreign government or the public, by causing serious harm to people or property, creating a serious risk to the health and safety to the public, or seriously disrupting trade, critical infrastructure or electronic systems (*Criminal Code Act 1995 (Cwlth)*) (National Counter-Terrorism Committee 2005, p. 2.2).

Terrorist Incident	a ‘terrorist incident’ is a combination of circumstances or conditions which may lead to or result from a terrorist act, and which require preventative and/or responsive action (National Counter-Terrorism Committee 2005, p. 2.2).

REFERENCES

AMCRAN (2005) Confusion reigns over terror laws. *AMCRAN media release* 2 July 2005.

Archbold, C. A. (2004) *Police accountability, risk management, and legal advising*. LFB Scholarly Publishing LLC, New York.

Archbold, C. A. (2005) Managing the bottom line: risk management in policing. *Policing: An International Journal of Police Strategies & Management, 28 (1)*, 30-48.

Blair, I. (2005) The Richard Dimbleby Lecture 2005 by Sir Ian Blair QPM, 16 November 2005. Downloaded 30 June 2006 from <http://cms.met.police.uk/met/layout/set/print/content/view/full/2682>

Dixon, D. (1999) Issues in the legal regulation of policing. In D. Dixon (Ed.) *A culture of corruption: Changing an Australian Police Service*. Hawkins Press, Sydney, pp. 36-68.

Gilmartin, K (2003) The continuum of compromise. In Royal Canadian Mounted Police Office of Ethics & Integrity (2003) *Ethical deliberations for RCMP employees*. Royal Canadian Mounted Police Course Code 000166, revised 25 August 2003, pp. 125-130.

Gorta, A. (2002) Developing a corruption risk profile for the NSW Government sector. Paper presented at the International Institute for Public Ethics 2002 Biennial Conference, Brisbane Australia, 4-7 October 2002.

Gorta A. (2006) Corruption risk areas and corruption resistance. In C. Sampford, A. Shacklock, C. Connors, & F. Galtung. (eds) *Measuring corruption*. Ashgate Publishing Limited, Hampshire, England, pp. 203-219.

Her Majesty's Inspectorate of Constabulary (HMIC) (1999) *Police integrity: Securing and maintaining public confidence*. Her Majesty's Inspectorate of Constabulary, June 1999.

Her Majesty's Inspectorate of Constabulary (HMIC) (2006) *Raising the standard: A thematic inspection of professional standards.* Her Majesty's Inspectorate of Constabulary, June 2006.

Hocking, J. (2003) Australian terror laws: An historical critique. National forum: The war of terrorism and the rule of law. NSW Parliament House, Sydney, 10 November 2003.

Independent Commission Against Corruption (1996) *Practical Guide to Corruption Prevention* Module 2, June 1996.

Independent Commission Against Corruption (2002) *Do-it-yourself corruption resistance guide*. *A corruption resistance review initiative: Toolkit*, March 2002, pp. 16-17.

Independent Commission Against Corruption (2003) *Profiling the NSW public sector Functions, risks and corruption resistance strategies.* January 2003.

McClellan, J. P. (2006) Terrorism and the law. Paper presented at Supreme Court Twilight Seminar: The new anti-terrorism legislation, Sydney, 28 February 2006.

Miller, J. (2003) Police corruption in England and Wales: An assessment of current evidence. *Home Office Online Report 11/03*.

National Counter-Terrorism Committee (2005) *National Counter-Terrorism Plan*. Second Edition, September 2005.

NSW Legislative Assembly (1998) Police Legislation Amendment (Protective Security Group) Bill, Second Reading, *Hansard, 23 June 1998*, pp. 6254-6256.

NSW Legislative Assembly (1998) Police Legislation Amendment (Protective Security Group) Bill, Second Reading, *Hansard, 24 June 1998*, pp. 6449-6452.

NSW Legislative Assembly (2002) Terrorism (Police Powers) Bill, Second Reading, *Hansard, 19 November 2002*, p. 6978.

NSW Legislative Assembly (2002) Terrorism (Police Powers) Bill, Second Reading, *Hansard, 21 November 2002*, p. 7430.

NSW Legislative Assembly (2004) Crimes Legislation Amendment (Terrorism) Billl, Second Reading, *Hansard, 22 June 2004*, p. 9851.

NSW Legislative Assembly (2005) Terrorism Legislation Amendment (Warrants) Bill, Second Reading, *Hansard, 9 June 2005*, p. 16940.

NSW Legislative Assembly (2005) Terrorism Legislation Amendment (Warrants) Bill, Second Reading, *Hansard, 10 June 2005*, p. 16949.

NSW Legislative Assembly (2005) Terrorism (Police Powers) Amendment (Preventative detention) Bill, Second Reading, *Hansard, 17 November 2005*.

NSW Legislative Council (1998) Police Legislation Amendment (Protective Security Group) Bill, Second Reading, *Hansard, 24 June 1998*, pp. 6377-6382.

NSW Legislative Council (2002) Terrorism (Police Powers) Bill, Second Reading, *Hansard, 3 December 2002*, p. 7623.

NSW Legislative Council (2002) Terrorism (Police Powers) Bill, Second Reading, *Hansard, 4 December 2002*, p. 7678.

NSW Legislative Council (2004) Crimes Legislation Amendment (Terrorism) Billl, Second Reading, *Hansard, 24 June 2004*, p. 10112.

NSW Legislative Council (2005) Terrorism Legislation Amendment (Warrants) Bill, Second Reading, *Hansard, 22 June 2005*, p. 17153.

NSW Legislative Council (2005) Terrorism (Police Powers) Amendment (Preventative detention) Bill, Second Reading, *Hansard, 30 November 2005.*

NSW Police (1999) *NSW Police Annual Report 1998-1999*, October 1999.

NSW Police (2000) *NSW Police Annual Report 1999-2000*, November 2000.

NSW Police (2001) *NSW Police Annual Report 2000-2001*, October 2001.

NSW Police (2002) *NSW Police Annual Report 2001-2002*, October 2002.

NSW Police (2003) *NSW Police Annual Report 2002-2003*, October 2003.

NSW Police (2004) *NSW Police Annual Report 2003-2004*, October 2004.

NSW Police (2005) *NSW Police Annual Report 2004-2005*, October 2005.

NSW Police (undated) Protective Security Group Charter (Abridged Version). (Copy provided to the Police Integrity Commission 26 May 2000.)

NSW Police Service (2000) Protective Security Group Operations Manual. NSW Police Service, February 2000.

NSW Police Service (Undated) Counter Terrorist Co-Ordination Command Induction Program. (Copy provided to the Police Integrity Commission 20 April 2006 and 26 June 2006.)

NSW Treasurer (2006) Budget Speech 2006-07. Delivered in the NSW Legislative Assembly on 6 June 2006. Downloaded 7 June 2006 from <http://www.treasury.nsw.gov.au/bp06-07/bp1/bp1.htm>

NSW Treasury (2006) *Budget Paper No. 3: 2006-07*. June 2006. Downloaded 7 June 2006 from <http://www.treasury.nsw.gov/bp06-07/bp3/bp3.htm>

Parliament of New South Wales Committee on the Office of the Ombudsman and the Police Integrity Commission (2004) Committee Inquiry: Police Integrity Commission oversight of NSW Police. *Media Release*, *26 February 2004*.

Parliament of New South Wales Committee on the Office of the Ombudsman and the Police Integrity Commission (2005) *Interim report on an inquiry into the Police Integrity Commission's jurisdiction to oversight the Protective Security Group*. Report No. 8/53 – March 2005.

Parliament of New South Wales Legislation Review Committee (2004) *Legislation Review Digest No 10 of 2004*, 30 August 2004, pp. 26-36

Parliament of New South Wales Legislation Review Committee (2005) *Legislation Review Digest No 8 of 2005*, 20 June 2005, pp. 33-45.

Parliament of New South Wales Legislation Review Committee (2005) *Legislation Review Digest No 15 of 2005*, 29 November 2005, pp. 20-39.

Police Integrity Commission (1998) *Report to Parliament regarding the Former Special Branch of the New South Wales Police Service*, June 1998.

Police Integrity Commission (2001) *Annual Report 2000-2001,* October 2001.

Police Integrity Commission (2002) *Annual Report 2001-2002,* October 2002.

Police Integrity Commission (2004) *Annual Report 2003-2004,* October 2004.

Premier of NSW (2002) Counter Terrorism Coordination Command. *Premier of New South Wales, News Release, 30 October 2002.*

Prenzler, T. (2002) Corruption and reform: Global trends and theoretical perspectives. In T. Prenzler & J. Ransley (Eds) *Police reform: Building integrity*. Hawkins Press, Sydney, pp. 3-23.

Privacy Committee (1978) The Special Branch: Criminal Records in NSW. Privacy Committee, March 1978.

Public Accounts Committee, NSW Parliament (2005) Risk management in the NSW Public Sector. *NSW Parliament, Legislative Assembly, Public Accounts Committee report, Report No. 12/53 (No. 155), September 2005*.

Punch, M. (2000) Police corruption and its prevention. *European Journal on Criminal Policy and Research, 8(3)*, 301-324.

Quinton, P., & Miller, J. (2003). Promoting ethical policing: Summary findings of research on new misconduct procedures and police corruption. *Home Office Online Report 12/03*.

Standards Australia (2003) *Fraud and corruption control. Australian Standard AS 8001-2003.*

Standards Australia & Standards New Zealand (2004a) *Risk Management. Australian Standard/New Zealand Standard 4360:2004*.

Standards Australia & Standards New Zealand (2004b) *Risk Management Guidelines Companion to AS/NZS 4360:2004.* Australian Standard/New Zealand Standards Handbook HB 436:2004.

Wheeler, J. (2005) *An independent review of airport security and policing for the government of Australia*. Australian Government: Airport and Policing Review.

Wood, J. J. R. T. (1997) *Royal Commission into the New South Wales Police Service. Final Report Volume II: Reform*, May 1997.

Wood, J. J. (2005) Judgment in *Regina v Zaky Mallah*. Supreme Court of NSW Common Law Division, Friday 11 February 2005.

APPENDIX 1: ROLE AND FUNCTIONS OF THE POLICE INTEGRITY COMMISSION

The Commission was established under the *Police Integrity Commission Act 1996* ('the Act') on the recommendation of the Royal Commission into the NSW Police Service. The principal functions of the Commission, set out in section 13 of the Act, are:

a. to prevent serious police misconduct and other police misconduct,

b. to detect or investigate, or manage other agencies in the detection or investigation of, serious police misconduct,

c. to detect or investigate, or oversee other agencies in the detection or investigation of, other police misconduct, as it thinks fit,

d. to receive and assess all matters not completed by the Police Royal Commission, to treat any investigations or assessments of the Police Royal Commission as its own, to initiate or continue the investigation of any such matters where appropriate, and otherwise to deal with those matters under this Act, and to deal with records of the Police Royal Commission as provided by this Act.

Other functions of the Commission in regard to police activities and education programs are set out in section 14 of the Act.[31] These include:

a. to undertake inquiries into or audits of any aspect of police activities for the purpose of ascertaining whether there is police misconduct or any circumstances that may be conducive to police misconduct,

b. in particular, to monitor the quality of the management of investigations conducted within NSW Police and to undertake audits of those investigations,

c. to make recommendations concerning police corruption education programs, police corruption prevention programs, and similar programs, conducted within NSW Police or by the Ombudsman or the Independent Commission Against Corruption for NSW Police, and,

d. to advise police and other authorities on ways in which police misconduct may be eliminated.

As far as practicable, the PIC is required to turn its attention principally to serious police misconduct (sub-section 13(2) of the Act).

31 Further functions of the Commission are set out in section 14A (functions relating to the special audit of the reform process) and section 15 (functions relating to the collection of information and evidence) of the Act.

POLICE MISCONDUCT

The expressions 'police misconduct' and 'serious police misconduct' are not explicitly defined by the Act. They nevertheless include the following types of conduct (see sub-section 5(2)):

(a) police corruption

(b) the commission of a criminal offence by a police officer

(b1) misconduct in respect of which the Commissioner of Police may take action under Part 9 of the *Police Act 1990*

(c) corrupt conduct within the meaning of the *Independent Commission Against Corruption Act 1988* involving a police officer

(d) any other matters about which a complaint can be made under the *Police Act 1990.*

It follows that 'police misconduct' may encompass not only serious criminal activity such as perverting the course of justice but also minor disciplinary breaches, the sanction for which may, for example, be nothing more than additional training and development.

ACQUIRING INFORMATION

The Commission has a wide range of means at its disposal for acquiring information. In addition to research of material in the public domain and audits or inquiries into police activities, in matters where the Commission determines to carry out an investigation it has special powers to:

- require public officials and public authorities to produce statements of information (section 25)
- require any person (whether or not a public official or public authority) to produce documents or other things (section 26)
- enter public premises (section 29)
- obtain search warrants (section 45)
- obtain warrants under the *Telecommunications (Interception) Act 1979*
- obtain warrants under the *Listening Devices Act 1984* (section 50 of the Act), and
- require persons to attend and give evidence or produce documents or other things before a hearing of the Commission, either in public or in private (section 38).

The Commission may conduct an investigation even though no particular police officer or other person has been implicated and even though no police misconduct is suspected (section 23(2)). Further, the Commission is not bound by the rules or

practice of evidence, and can inform itself on any matter by means it considers appropriate (section 20(1)). Such means might include, for example, interviews, focus groups or private hearings with experts, police officers or others. These might be conducted for the purposes of gathering information which is relevant to NSW Police policies and procedures or other topics bearing on the prevention of police misconduct, circumstances conducive to police misconduct, or other matters related to the Commission's functions.

REPORTS TO PARLIAMENT

WHEN DOES THE COMMISSION SUBMIT A REPORT TO PARLIAMENT?

The Commission may prepare a report to Parliament in relation to any matter that is or has been the subject of an investigation (sub-section 96(1)). The Commission may also make a special report on any administrative or general policy matter relating to the functions of the Commission (section 98). A report to Parliament must be provided to the Presiding Officer of each House of Parliament as soon as possible after the Commission has concluded its involvement in the matter, unless it is considered desirable, in the public interest, for the making of the report to be deferred (sub-sections 96(4) and (5)). Where the Commission has conducted a public hearing for the purpose of an investigation, it must prepare a report to Parliament on that matter (sub-section 96(2)).

WHAT IS INCLUDED IN A REPORT TO PARLIAMENT?

The contents and structure of a report to Parliament will vary according to whether it reports on an investigation, an audit, another type of inquiry or a combination of these. Generally, a report will first present the relevant information and/or evidence acquired. The Commission assesses this information to reach opinions on whether there is or has been police misconduct or any circumstances that may be conducive to police misconduct. On the basis of the Commission's assessments, the report may include a number of recommendations (sub-sections 16(1) and 97(1)). These may include recommendations as to whether consideration should or should not be given to the prosecution of persons (including police officers) for criminal or disciplinary[32] offences and, in the case of police officers, other forms of disciplinary action (sub-section 16(1)(b), sub-section 97(2)). Opinions and recommendations regarding individuals are discussed further in the following section.

The Commission may also recommend other measures which it considers should be taken in relation to its opinions and assessments (sub-section 16(1)(c)). Such recommendations may relate, for example, to law reform or to changes in NSW Police policies and procedures which impact on the prevention or detection of misconduct or on circumstances which are conducive to misconduct.

[32] While the Act refers to 'disciplinary offences', this definition no longer applies in practice to police officers. The power of the Commissioner of Police to refer a departmental charge against a police officer for a disciplinary offence was repealed on 8 March 1999. Since that date, the powers and obligations of the Commission to recommend whether consideration should be given to the prosecution of an officer for a specified 'disciplinary offence' (sections 16(1)(b), 97(2)(b)) has no effective application to police officers. This is so even for police misconduct that occurred before this date. Those powers and obligations may, however, have application to other public officials.

OPINIONS AND RECOMMENDATIONS REGARDING INDIVIDUALS

Assessments and opinions about misconduct

The standard of proof applied by the Commission to the formation of an opinion as to whether a person has engaged in police misconduct or other misconduct is the balance of probabilities. Such an opinion will be reached having regard to the principles in *Briginshaw v Briginshaw* (1938) 60 CLR 336. That is, the more serious the matters under consideration, the more stringent will be the requisite degree of satisfaction.

The Commission may form opinions as to whether police misconduct or other misconduct has or may have occurred, is or may be occurring, is or may be about to occur, or is likely to occur (sub-section 16(1)(a)). However, it is important to bear in mind that the Commission is an investigative agency, it is not a court or tribunal and may not make a finding or form an opinion that a specified person is guilty of or has committed, is committing or is about to commit an offence (sub-section 16(2)(a)). Accordingly the Act deems permissible opinions concerning police misconduct or other misconduct not to be findings or opinions that the person is guilty of or has committed, or is committing or is about to commit a criminal offence (subsection 16(3)). That said, the Commission recognises, bearing in mind the definition of police misconduct may include conduct that amounts to criminal and disciplinary offences, that such opinion may in some circumstances take on the appearance of a finding of a court or a tribunal. The Commission's approach is, as far a possible, to avoid the expression of opinions that may be characterised as findings by a court.

Recommendations to consider prosecution

If, in the Commission's opinion, the available evidence is sufficient to establish a prima facie case in respect of a criminal offence then it is generally the practice of the Commission to recommend that consideration be given to the prosecution of a person for a specified criminal offence. Such a recommendation will be made to the relevant prosecutorial authority, for example, the New South Wales Office of the Director of Public Prosecutions. In deciding whether to make such a recommendation, the Commission generally does not have regard to discretionary considerations, such as whether there is a reasonable prospect of conviction.[33] These and other discretionary considerations are appropriate matters for the relevant prosecutorial authority. That said, the Commission may make findings or express opinions as to the veracity of evidence received from individual witnesses.

Recommendations regarding action against 'Affected Persons' and others

The Act defines an 'affected person' as a person against whom, in the Commission's opinion, substantial allegations have been made in the course of, or in connection with, the investigation (sub-section 97(3)). Where the Commission reports to Parliament on an investigation involving affected persons, the report must include a statement as to whether or not the Commission is of the opinion that consideration should be given to prosecution of the person for a specified criminal or disciplinary offence and, if the person is a police officer, whether consideration should be given to:

---

33 The only circumstance in which the Commission may, despite the existence of a prima facie case against a person, decide not to recommend that consideration be given to their prosecution is where it considers that to do so would be inconsistent with the functions of the Commission.

- action against the person as a police officer on specified grounds (including action for the loss of the Commissioner's confidence under section 181D of the *Police Act 1990*) with a view to dismissing or otherwise terminating the services of the police officer (sub-section 97(2)(c))
- 'reviewable action' under section 173 of the *Police Act 1990* against the police officer (sub-section 97(2)(d)).

'Reviewable action' within the meaning of section 173 of the *Police Act 1990* refers to forms of disciplinary action that would ordinarily apply to more serious breaches of discipline. The available forms of reviewable action are:

- a reduction in a police officer's rank or grade
- a reduction in the police officer's seniority
- a deferral of the police officer's salary increment, and
- any other action (other than dismissal or the imposition of a fine) that the Commissioner of Police considers appropriate.

These types of action are reviewable, since, owing to their seriousness, a police officer may appeal the imposition of any of these penalties to the Industrial Relations Commission of New South Wales.

The Commission may also recommend that prosecution or (in the case of a police officer) any of the disciplinary actions above be considered in the case of a person who is not an 'affected person' (sub-section 97(4)).

For both 'affected persons' and any other persons, the Commission may also recommend the consideration of other disciplinary actions (sub-section 97(4)). Such actions may include 'non-reviewable action' within the meaning of section 173 of the *Police Act 1990*. Non-reviewable action would generally apply to less serious breaches of discipline. There is no avenue of appeal to the Industrial Relations Commission against the imposition of a form of non-reviewable action. The available forms of non-reviewable action are:

- coaching
- mentoring
- training and development
- increased professional, administrative or educational supervision
- counselling
- reprimand
- warning
- retraining
- personal development
- performance enhancement agreements

- non-disciplinary transfer
- change of shift (but only if the change results in no financial loss and is imposed for a limited period and is subject to review)
- restricted duties, and
- recording of adverse findings.

APPENDIX 2: CHRONOLOGY

1948	Special Branch commenced operation.
12 March 1997	Commissioner of NSW Police disbanded the Special Branch and secured its records following evidence put before the Royal Commission into the NSW Police Service of abuses of power and a lack of accountability in the operations of Special Branch. The administrative positions were relocated to VIP Security Unit.
May 1997	Report of the Royal Commission into the NSW Police Service released. This report documented a number of 'matters of serious concern' regarding the operations of Special Branch. (For further information see Section 2.1 in Chapter 2 of this report.)
17 June 1998	Police Integrity Commission released its 'Report to Parliament regarding the Former Special Branch of the NSW Police Service'. This report includes adverse comments regarding a number of Special Branch practices. (For further information see Section 2.1 in Chapter 2 of this report.)
10 July 1998	*Police Legislation Amendment (Protective Security Group) Act 1998* (NSW) commenced. (Assented to 2/7/1998.) This Act established the regime required to oversight the Protective Security Group. (For further information see Section 2.2 of this report.)
10 August 1998	VIP Security Unit renamed as Protective Security Group.
13 May 1999	The Commission received a copy of the NSW Police first annual audit of the Protective Security Group. This audit report covered the period July 1998 to April 1999.
23 August 1999	The Commission received a Supplementary Audit report from NSW Police on the operations of the Protective Security Group for the period July 1998 to April 1999.
4 May 2000	The Commission received a copy of the NSW Police audit of the Protective Security Group for the 1999 calendar year.
April 2001	The Commission received a copy of the NSW Police audit of the Protective Security Group for 2000.
11 September 2001	Attacks on the World Trade Centre in New York City and the Pentagon in Washington.
October 2001	The Commission reported on the NSW Police 1998, 1999 and 2000 audits of the Protective Security Group in its 2000-01 Annual Report.

July 2002	The Commission received a report of the NSW Police audit of the Protective Security Group for 2001.
12 October 2002	Bombings in Bali.
24 October 2002	Inter-governmental Agreement on Australia's National Counter-Terrorism Arrangements.
29 October 2002	NSW Police Counter-Terrorist Co-ordination Command created.
13-15 November 2002	First meeting of National Counter-Terrorism Committee (which replaced the Standing Advisory Committee for Commonwealth/State Co-operation for the Protection Against Violence (SAC-PAV)).
13 December 2002	*Terrorism (Commonwealth Powers) Act 2002* (NSW) introduced to refer certain matters relating to terrorist acts to the Commonwealth Parliament in accordance with the Commonwealth Constitution, so as to enable the Commonwealth Parliament to make laws about those matters.
13 December 2002	*Terrorism (Police Powers) Act 2002* (NSW) commenced. (assented to 5/12/2002) to confer special powers [to obtain disclosure of identify, to search persons, to search vehicles, to enter and search premises, to seize and detain things] on police officers to deal with imminent threats of terrorist acts and to respond to terrorist acts. (For further information see Chapter 3 and Appendix 3.)
December 2002	The Commission received a report of the NSW Police Special Review of the Protective Security Group.
17 March 2003	Functions of the Protective Security Group were absorbed into the Counter Terrorist Coordination Command.
August 2003	NSW Police Audit Group, Protective Security Group Audit (2002) report prepared.
December 2003	The Commission received a report of the NSW Police audit of the Protective Security Group for 2002.
25 February 2004	Parliamentary Committee on the Office of the Ombudsman and the Police Integrity Commission Inquiry into the Police Integrity Commission's jurisdiction to oversight the Protective Security Group (date referred). The Terms of Reference specified that this was an inquiry into: a. the functions of the PIC under ss. 14(e)-(f) of the *Police Integrity Commission Act 1996* b. the provision of reports to the PIC under Part 3 of the *Police Act 1990* c. oversight of the conduct of NSW Police officers

	involved in the Counter Terrorism Coordination Command (CTCC), and d. any other matter that the Committee considers relevant to the inquiry. (For further information see Section 2.4 in Chapter 2 of this report.)
11 March 2004	Bombing of Madrid commuter trains.
27 May 2004	Public Hearing conducted by the Parliamentary Committee on the Office of the Ombudsman and the Police Integrity Commission into the Police Integrity Commission's jurisdiction to oversight the Protective Security Group. (For further information see Section 2.4 in Chapter 2 of this report.)
4 June 2004	*Bail Amendment (Terrorism) Act 2004* assented to and commenced. This Act amended the *Bail Act 1978* to create a presumption against bail in respect of person charged with certain terrorism offences under the *Commonwealth Criminal Code 1995*.
6 July 2004	*Crimes Legislation Amendment (Terrorism) Act 2004* – Schedule 3 (Amendment of Terrorism (Police Powers) Act 2002) assented to and commenced. Schedule 3 sought to clarify the circumstances in which the special powers may be authorised as well as to authorise police officers to give directions to government agencies for the purpose of exercising police special powers and to enable officers to place a cordon around a target area. (For further information see Chapter 3 and Appendix 3.)
12 August 2004	The Commission made submission to Parliamentary Committee Inquiry that the Commission conduct this risk assessment. (For further information see Section 2.4 in Chapter 2 of this report.)
9 September 2004	Bombing of Australian Embassy, Jakarta.
October 2004	The Commission reported on the NSW Police 2000, 2001 annual audits and the NSW Special Review of the Protective Security Group in its 2003-04 Annual Report.
22 March 2005	Parliamentary Committee on the Office of the Ombudsman and the Police Integrity Commission tabled its 'Interim Report on an Inquiry into the Police Integrity Commission's jurisdiction to oversight the Protective Security Group'. (For further information see Section 2.4 in Chapter 2 of this report.)
7 July 2005	Bombings of London underground rail network and a bus.
September 2005	*Terrorism Legislation Amendment (Warrants) Act 2005* (NSW)

	• Schs 1 and 2 commenced 13/9/2005 • Sec 2(1) commenced 9/9/2005 • Sec 6 scheduled to commence on 13/9/2007 (Act assented to 27/6/2005). This Act enabled 'eligible officers' to enter, without any occupier's knowledge, and search premises under authority of a special covert search warrant. (For further information see Chapter 3 and Appendix 3.)
1 October 2005	Second wave of bombings of Bali holiday venues.
16 December 2005	*Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005* (NSW) commenced 16/12/2005. This Act enables a person to be taken into custody and detained for a short period of time to prevent an imminent terrorist act or to preserve evidence of, or relating to, a recent terrorist act. (For further information see Chapter 3 and Appendix 3.)
12 February 2006	Official commencement date of Public Order and Riot Squad (PORS).
29 March 2006	Parliamentary Committee on the Office of the Ombudsman and the Police Integrity Commission established Inquiry into (a) the functions of the PIC and the Ombudsman under the counter-terror laws of NSW and in relation to oversight of the police use of covert and coercive powers; (b) oversight of the conduct of NSW police officers involved in the Counter Terrorism Coordination Command (CTCC); (c) trends in anti-terror laws and oversight of these extraordinary powers; d) impact of the growth of police powers on the nature of external police oversight; (e) any other matter that the Committee considers relevant to this inquiry. (For further information see Section 2.4 in Chapter 2 of this report.)
12 July 2006	Bombing of rail network in Mumbai, India.

APPENDIX 3: SUMMARY OF SELECTED LEGISLATIVE PROVISIONS IN RELATION TO TERRORISM

A3.1: INTRODUCTION

BACKGROUND

A summit of Commonwealth and State and Territory leaders (Leaders' Summit on Transnational Crime and Terrorism), held in Canberra on 5 April 2002, resulted in State governments referring their powers over terrorism to the Commonwealth. The Commonwealth *Criminal Code Amendment (Terrorism) Act 2003* provides for the Commonwealth to legislate in this area, with agreement from the States for future amendments. At the State level, NSW introduced the *Terrorism (Commonwealth Powers) Act 2002* in December 2002 to refer certain matters relating to terrorist acts to the Commonwealth Parliament in accordance with section 51 (xxxvii) of the Commonwealth Constitution, to enable the Commonwealth Parliament to make laws about these matters.

As a result, while many laws have been enacted to combat terrorism at the Commonwealth level, there is relatively little State or Territory legislation relating to counter-terrorism. The Australian Government National Security website[34] states that the Australian Government has introduced an extensive legislative regime around counter-terrorism, national security and other cross-jurisdictional offences and lists the 'key pieces of Australia's national security legislation', which numbered 29 Acts and amendment Acts in late May 2006.

PURPOSE OF THIS APPENDIX

Rather than seeking to review the provisions of each piece of counter-terrorism legislation, this appendix focuses on NSW counter-terrorism legislation which affects police powers. Hence it focuses on the *Terrorism (Police Powers) Act 2002* (discussed in Section A3.2 of this appendix) and its subsequent amendments:

- *Crimes Legislation Amendment (Terrorism) Act 2004* (see Section A3.3 of this appendix)
- *Terrorism Legislation Amendment (Warrants) Act 2005* (see Section A3.4), and
- *Terrorism Legislation Amendment (Preventative Detention) Act 2005* (see Section A3.5).

This Appendix does not seek to provide a comprehensive outline of all aspects of this legislation. Instead, it focuses on NSW Police powers and accountability requirements provided within the legislation.

Table 3.1, in Chapter 3, provides an overview for this legislation of:

[34] <www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf>

- the dates of commencement
- powers provided for NSW Police
- the conditions under which these powers can be used
- who authorises these powers
- which officers can employ the powers, and
- the accountability requirements associated with each of these Acts.

The following sections of this appendix provide a separate summary, for each of the four pieces of legislation, of: the object, police powers, authorisation process, limitations, and accountability requirements attached to these selected legislative provisions. Each section also includes relevant extracts concerning any accountability and oversight issues raised in the second reading speech and associated parliamentary debates. These summaries are based on a consideration of the legislation, explanatory notes to the bills, second reading speeches and associated parliamentary debates, and issues raised by the Legislative Review Committee.

A3.2: TERRORISM (POLICE POWERS) ACT 2002

OBJECT

To confer special powers [to obtain disclosure of identify, to search persons, to search vehicles, to enter and search premises, to seize and detain things] on police officers to deal with imminent threats of terrorist acts and to respond to terrorist acts.

The Commissioner of Police (or other senior police officer) may, with the concurrence or confirmation of the Police Minister, give an authorisation for the exercise of those special powers:

a. for the purpose of finding a particular person named or described in the authorisation (the *target person*), or

b. for the purpose of finding a particular vehicle, or a vehicle of a particular kind, described in the authorisation (the *target vehicle*), or

c. for the purpose of preventing or responding to a terrorist act in a particular area described in the authorisation (the *target area*).

The authorisation enables a police officer to demand that a person give his or her name and address (and to request proof of identity) if the officer reasonably suspects that the person is the target person (or in his or her company), is in the target vehicle or is in the target area (including entering or having just left the target area). Such a person is also liable to be searched without warrant, as is any vehicle that the officer reasonably suspects contains the target person, or is the target vehicle or that is in the target area. An authorisation also permits a police officer to enter and search, without warrant, any premises that he or she reasonably suspects contains a target person or target vehicle or that are in the target area.

In relation to any search, a police officer is authorised to seize and detain anything that the officer suspects on reasonable grounds may be used or may have been used to commit a terrorist act or may provide evidence of the commission of a serious indictable offence.

The Act also amends the *State Emergency and Rescue Management Act 1989* to give additional powers to a police officer to quarantine a person who may have been exposed to chemical, biological or radiological contamination and to direct the person to undergo decontamination procedures. Police officers are also given powers to remove a vehicle from a danger area and to prevent a person from interfering with objects in, or removing objects from, a danger area.

COMMENCEMENT DATE

Assented to on 5 December 2002 and commenced on 13 December 2002.

SPECIAL POWERS

Following authorisation, the following powers may be exercised by any police officer (s. 14(1)):

- *To obtain disclosure of identity* - A police officer may require a person to disclose his or her identity if the officer suspects on reasonable grounds that the person is the target person (or the person is found in suspicious circumstances in the company of the target person), is on or in a vehicle that the officer suspects on reasonable grounds is the target vehicle, or is in the target area. The officer may also request the person to provide proof of his or her identity (s. 16).
- *To search persons* - A police officer may, without a warrant, stop and search a person, or anything in the person's possession or control, if the officer suspects on reasonable grounds that the person is the target person (or the person is found in suspicious circumstances in the company of the target person), the person is on or in a vehicle that the officer suspects on reasonable grounds is the target vehicle or the person is in the target area (s. 17).
- *To search vehicles* - A police officer may, without a warrant, stop and search a vehicle and anything on or in the vehicle if the officer suspects on reasonable grounds that the vehicle is the target vehicle or the officer suspects on reasonable grounds that a person on or in the vehicle is the target person or the vehicle is in the target area (s. 18).
- *To enter and search premises* - A police officer may, without a warrant, enter and search any premises if the officer suspects on reasonable grounds that the target person, or the target vehicle, may be in the premises or the premises are in the target area (s. 19).
- *To seize and detain things* - A police officer may seize and detain anything that the officer suspects on reasonable grounds may be used or may have been used to commit a terrorist act or may provide evidence of the commission of a serious indictable offence (whether or not related to a terrorist act). The power to seize and detain a thing includes a power to guard the thing and a power to remove the thing (s. 20).
- *To use reasonable force* - A police officer, and any person helping the police officer, is permitted to use reasonable force in the exercise of these special powers (s. 21).

AUTHORISATION

The exercise of special powers may be authorised only where the police officer giving the authorisation is satisfied that there are reasonable grounds for believing that:

a. there is an imminent threat[35] of a terrorist act and that the exercise of the powers will substantially assist in preventing the terrorist act (s. 5), or

[35] 'Imminent threat' was amended by the *Crimes Legislation Amendment (Terrorism) Act 2004* which is discussed later in this appendix.

b. a terrorist act has been committed and that the exercise of the powers will substantially assist in apprehending the persons responsible for committing the terrorist act (s. 6).

An authorisation may be made by the Commissioner of Police or a Deputy Commissioner of Police. However, if those officers are not able to be contacted and the authorisation is sought urgently, then the authorisation may be given by any officer above the rank of superintendent (s. 8).

An authorisation must be given with the concurrence of the Police Minister unless he or she is not able to be contacted, in which case the authorisation may be given without concurrence, but must be notified to the Police Minister as soon as he or she is available (s. 9). If an authorisation is given under section 5 of the Act without concurrence of the Police Minister, it ceases to have effect after 48 hours if it is not confirmed by the Police Minister within that time (s. 9).

LIMITATIONS

- An authorisation has effect for the time specified in the authorisation unless sooner revoked. An authorisation under section 5 has a maximum duration of 7 days and may be extended, with the concurrence of the Police Minister, up to a maximum total period of 14 days. An authorisation under section 6 has a maximum duration of 24 hours and may be extended, with the concurrence of the Police Minister, up to a maximum total period of 48 hours (s. 11).
- The Police Minister may at any time direct that an authorisation be revoked (s. 12 (1)).
- A strip search may only be carried out on someone suspected to be the target and who is aged ten years or older (Schedule 1 [7]). Searches are otherwise limited to ordinary searches and frisk searches (s. 17 (2), also see Schedule 1 [3] and [4]).
- A police officer entering and searching any premises under the Act must do as little damage as possible (s. 19 (2)).

ACCOUNTABILITY

- An authorisation may be given orally but must be confirmed in writing as soon as is reasonably practicable. The authorisation must specify that it is made under the Act, describe the general nature of the terrorist act to which it applies, name or describe the person, vehicle or area targeted and specify the time that the authorisation ceases to have effect (s. 10).
- The validity of an authorisation is reviewable by the Police Integrity Commission (s. 13). (The Ombudsman's jurisdiction to oversight complaints about the inappropriate exercise of the powers is not affected.)
- If requested to do so, a police officer must provide certain information to the person subject to the exercise of a special power. This includes evidence that the police officer is a police officer, the name of the police officer and his or her place of duty, and the reason for the exercise of the power. The Commissioner of Police must also arrange for a written

statement to be provided, on request made within 12 months of the search, to a person who was searched, or whose vehicle or premises were searched, under this Act (s. 23).

- The Commissioner of Police must provide a report to the Attorney General and the Police Minister as soon as practicable after the expiry of an authorisation, setting out the terms and period of the authorisation, identifying as far as reasonably practicable the matters that were relied on for giving the authorisation, describing the powers exercised and specifying the results of the exercise of those powers (s. 26, subsequently renumbered as s. 14B).
- A Ministerial review of the Act is to be undertaken 12 months after the date of assent and every 12 months thereafter. A report on the outcome of each review is to be tabled in Parliament within 12 months after the end of each period (s. 36).

ISSUES RAISED IN SECOND READING SPEECH & ASSOCIATED PARLIAMENTARY DEBATES[36]

In introducing this legislation the former Premier, Mr Carr, described both the limitations to the circumstances in which the powers can be used as well as the need for checks and balances:

> The new powers given to police are confined to limited circumstances. As I have said repeatedly, it is not my instinct to fling at police and security agencies crudely increased powers. In any democracy there must be a healthy suspicion of law enforcement powers. We must carefully monitor their use. We have time-limited the increased powers and created a special trigger before they can be invoked. That is an alternative model to just saying that police shall have these extra powers to search, and to do so in all these circumstances.
>
> We are not doing that. We are saying that where there is a credible terrorist threat, or where there has been an actual incident, for a period of seven days and two days respectively police will enjoy these increased powers. Then the powers automatically lift unless they are specifically renewed. That is a time limit on these powers. It is a check. It is a balance. Moreover, we are making sure that in these areas – as in all areas – the police and their behaviour are subjected to the oversight of the Police Integrity Commission and the Ombudsman. So there will be that review capacity, as there ought to be. We want accountability to apply even where police are responding to terrorism. …
>
> The new powers are not intended for general use. In ordinary circumstances we rely on standard police investigations and the co-operation of Australian and international law enforcement and intelligence agencies. However, when an attack is imminent, all resources must be able to be mobilised with maximum efficiency. Similarly, when an attack has just occurred, there is an increased chance of catching the terrorists, and this chance must be seized. …
>
> Legitimate, non-violent protest cannot trigger the proposed powers. …

[36] NSW Legislative Assembly Hansard, 19 November 2002, 21 November 2002; NSW Legislative Council Hansard, 3 December 2002, 4 December 2002.

> Clause 13 makes it clear that the decisions of senior police are reviewable by the Police Integrity Commission. The Ombudsman's jurisdiction to oversight complaints about the inappropriate exercise of the powers under the bill is not affected (NSW Legislative Assembly Hansard, 19 November 2002).

Mr Barr, the member for Manly, raised his concern as to whether the proposed powers can be used to oppress legitimate political dissent:

> A major concern is whether this bill can be used as an instrument to oppress legitimate political dissent or particular groups in the community. The definition of 'terrorism' is quite wide and not that clear. To fall within the scope of the bill the action must be intended to coerce the government and advance a political, religious or ideological cause. It must also cause serious harm or risk of harm to persons, property or an electronic system, such as telecommunications. It is not clear what action will be deemed as causing serious harm. Action deemed to be advocacy, protest, dissent or industrial action is excluded from the bill if it is not intended to cause serious harm or risk to persons – property does not count. Therefore it would appear possible for these forms of action to be included in the scope of the bill if it is found that intention to cause harm to persons existed. The intent element may become contentious in the case of a spontaneous protest action that turns violent. It is arguable that the powers in the bill could be invoked during such a protest if intent were proven. The fact that authorisation under the Act is not open to challenge makes the potential for the power to be abused in this way something of a concern (NSW Legislative Assembly Hansard, 21 November 2002).

Following the second reading in the Legislative Council, the Hon. Helen Sham-Ho raised specific concerns regarding the lack of judicial oversight provided in clause 13:

> The Law Society is particularly troubled by the lack of judicial review under the bill, and referred to clause 13, which effectively states that an authorisation 'may not be challenged, reviewed, quashed or called into question … before any court, tribunal, body or person in any legal proceedings'.[37] The Law Society argues that immunity from judicial review is anti-democratic and strikes at the fundamental principle that the Government's actions should always be subject to judicial review. I strongly support the Law Society's objection to this clause.
>
> As it stands, clause 13 would vest entire and unfettered authority with the Government. This goes against the most basic tenets of our legal system, namely, the separation of powers doctrine. Without an avenue for judicial review, members of the Police Force will essentially be answerable only to themselves. … As I have said many times in this House, courts are the people's greatest watchdog over government. The judiciary must have an oversight role over these new police powers. Because I feel so strongly about this issue, I will move an amendment to remove clause 13 from the bill (NSW Legislative Council Hansard, 3 December 2002).

Ms Lee Rhiannon of the Greens also expressed concern about the removal of judicial oversight of the authorisation process. She said that:

> The Greens believe the Terrorism (Police Powers) Bill is unnecessary. … The Greens also believe that the bill unacceptably erodes our democratic

[37] Other than under the *Police Integrity Commission Act 1996*.

> freedoms. It runs counter to our commitment to an open, free and democratic society. It blurs the separation of powers by dangerously removing power from the judiciary and giving it to the Executive. Allowing Ministers to approve warrants and prohibiting any judicial oversight of the new powers are unacceptable erosions of our democratic freedoms. We do not believe that it is valid to defend democracy by dismantling it in this way (NSW Legislative Council Hansard, 3 December 2002).

The Hon. Peter Breen subsequently raised a related concern:

> The advice of the Crown Solicitor tabled by the Minister confirms the meaning of the words in the bill, namely that a legal proceeding under the Police Integrity Commission Act is an exception to the principle of special power in the hands of the commission and the Minister. But the Minister is not a police officer and the authority of the PIC to investigate would depend on the conduct complained of involving a police officer. The advice does not say whether the PIC could investigate a matter involving the misuse of executive power by the Minister for Police. This is the area of greatest concern … (NSW Legislative Council Hansard, 4 December 2002).

In response the Hon. Michael Costa, the then Minister for Police, said that the role of the Police Integrity Commission is much broader than investigating police officers and the Police Integrity Commission could in fact investigate the conduct of the Police Minister:

> I reiterate that the PIC has a broader scope to investigate than possessed by the Independent Commission Against Corruption. The PIC is not limited to investigating only police conduct. Section 130(2) of the Police Integrity Commission Act provides that the PIC may investigate and otherwise deal with a matter involving the conduct of public officials provided it is done in the context of matters that involve police officers. Clearly, the exercise of this power would do that. 'Public officials' has the same meaning as in the Independent Commission Against Corruption Act and includes a Minister of the Crown. Therefore, the PIC may, if it sees fit and in accordance with its functions under the Police Integrity Act, examine the Minister's decisions to concur with, confirm or revoke an authorisation (NSW Legislative Council Hansard, 4 December 2002).

The Hon. Richard Jones raised the issue that officers cannot be convicted or held liable merely because the person who gave the authorisation lacked the jurisdiction to do so:

> In other words, the authorisation cannot be contested except by the Police Integrity Commission, and if the authorisation has been given by someone who had no power to do so an officer acting on it cannot be held liable. Thus the citizens of New South Wales are at the whim of police officers, who effectively answer to no-one. … The bill takes away the rights of any member of the public to sue police who are acting pursuant to a purported authorisation, even if it turns out later that this authorisation did not exist (NSW Legislative Council Hansard, 3 December 2002).

OTHER

There is no Legislative Review Committee report considering the *Terrorism Police Powers Bill 2002*, since this Bill was introduced prior to the establishment of the Legislation Review Committee and the requirement for the Committee to consider and

report on any Bill introduced to NSW Parliament (as per s. 8A of the *Legislation Review Amendment Act 2002*).

A3.3: CRIMES LEGISLATION AMENDMENT (TERRORISM) ACT 2004

OBJECT

To make a number of miscellaneous amendments to the *Crimes Act 1900*,[38] the *Criminal Procedure Act 1986*,[39] the *Terrorism (Police Powers) Act 2002*[40] and the *State Emergency and Rescue Management Act 1989*[41] arising from a review of offences and powers relating to terrorism.

The amendments to the *Terrorism (Police Powers) Act 2002,* provided in Schedule 3, clarify the circumstances in which the special powers may be authorised, authorise the Commissioner of Police or a Deputy Commissioner (or other available senior police officer) to give directions to government agencies (and their members and officers) to facilitate the exercise of the special powers conferred on police officers when authority to exercise those powers has been given, and to place a cordon in or around a target area.

COMMENCEMENT DATE

Assented to on 6 July 2004 and Schedule 3 commenced on day of assent.

SPECIAL POWERS

- *To give directions to government agencies* - Gives authority to the Commissioner of Police or a Deputy Commissioner (or other available senior officer) to give directions to government agencies (and their members and officers) with respect to the exercise of the powers or functions of the agency for the purpose of facilitating the exercise of police special powers under the *Terrorism (Police Powers) Act 2002* (s. 14A).
- *To place a cordon around target area* - Confers a specific power on police officers to place a roadblock or other cordon in or around a target area where police officers are authorised to exercise special powers under the *Terrorism (Police Powers) Act 2002* to search persons, vehicles or premises (s. 19A).

AUTHORISATION

The authorisation process is the same as that described in the previous section on the *Terrorism (Police Powers) Act 2002*, other than now one part of the test is the requirement that the Commissioner of Police (or Deputy or other senior officer) is satisfied that there are reasonable grounds for believing that there is 'a threat of a terrorist act occurring in the near future', rather than believing that there is 'an imminent threat of a terrorist act' as was the case prior to this amendment. The second limb of the test in the *Terrorism (Police Powers) Act 2002* still remains. That is, the

[38] Amendments relate to poisoning, explosives and sabotage offences (Schedule 1).

[39] Amendment relates to the prosecution of new explosives offence (Schedule 2).

[40] These amendments, made in Schedule 3, are discussed in this appendix.

[41] Amendment includes "terrorist act" in the list of imminent occurrences that can constitute an emergency for the purposes of the Act (Schedule 4).

Commissioner (or other senior officer) must be satisfied that the exercise of the powers will substantially assist in preventing the terrorist act.

LIMITATIONS

Limitations are the same as those described in the previous section on the *Terrorism (Police Powers) Act 2002.*

ACCOUNTABILITY

Accountabilities are the same as those described in the previous section on the *Terrorism (Police Powers) Act 2002.*

ISSUES RAISED IN SECOND READING SPEECH & ASSOCIATED PARLIAMENTARY DEBATES[42]

When introducing this amendment, Mr Bob Debus (Attorney General and Minister for the Environment) stated that:

> Item [1] of schedule 3 amends the trigger at section 5 of the Act. This is the trigger for activating the powers in advance of a terrorist act. The Government's intention with this legislation is to give NSW Police the capacity to act when a senior and experienced officer, on the basis of the information available, and in light of that officer's experience, feels it is necessary to do so, in order to forestall a possible terrorist attack. …
>
> The type of information may not be exact, for example police may not necessarily have an understanding of the form the terrorist threat might take whether it is a car bomb, a suicide bombing or a shooting. The concern the police have must be based on evidence. The trigger does create a genuine test. But that test must have a relatively low threshold given the consequences if police do not act. ….
>
> These powers are extreme but so are the consequences of not acting when, as it were, the terrorists are in the home straight. The existing safeguards under the Act remain. The decision of senior police to activate the powers must be ratified by the Minister for Police. Similarly, when the powers are used, a report must be made by NSW Police to the Attorney General and the Minister for Police. The Act also has a built-in requirement that it be reviewed annually. The ongoing review of terrorism powers and the experience gained from counter-terrorism exercises also indicate that these additional amendments to the Act are needed (NSW Legislative Assembly Hansard, 22 June 2004).

ISSUES RAISED BY LEGISLATIVE REVIEW COMMITTEE[43]

The Legislative Review Committee concerned itself with issues pertaining to Schedule 1 (amendments to the *Crimes Act* pertaining to possession of explosives and the presumption of innocence). It did not raise any issues concerning the Schedule 3 amendments other than describing the nature of those amendments:

---

[42] NSW Legislative Assembly Hansard, 22 June 2004; NSW Legislative Council Hansard, 24 June 2004.

[43] Parliament of New South Wales Legislation Review Committee (2004) *Legislation Review Digest No 10 of 2004*, 30 August 2004, pp. 26-36.

> Section 5 previously provided that the special powers are only exercisable if the Commissioner or a Deputy Commissioner of Police (or other available senior police officer) is satisfied that there are reasonable grounds for believing that there is an ***imminent*** threat of a terrorist act. The Commissioner must also be satisfied that the exercise of these powers will substantially assist in preventing a terrorist act.
>
> The amendment broadens the circumstances in which the Commissioner may exercise these special powers by removing the requirement that the Commissioner be satisfied that the terrorist threat is imminent. Under the amended section 5, the Commissioner need only be satisfied of a threat *occurring in the near future*.
>
> The Commissioner must still, however, be satisfied that the exercise of those powers will substantially assist in preventing the terrorist act remain unaltered (p. 30).

OTHER

This amendment Act was repealed on 1 July 2005 by Schedule 3 to the *State Law (Miscellaneous Provisions) Act 2005.* It was repealed to rationalise the legislation in force on the basis that the amendments had commenced and the repeal has no substantive effect on the amendments made by the Act or any associated provisions.

A3.4: TERRORISM LEGISLATION AMENDMENT (WARRANTS) ACT 2005

OBJECT

To amend:

- the *Terrorism (Police Powers) Act 2002* to enable covert entry and search of premises, under the authority of a special covert search warrant, by specially authorised police officers or staff of the NSW Crime Commission for the purposes of responding to or preventing terrorist acts (including getting evidence of the State offence of membership of a terrorist organisation)

- the *Listening Devices Act 1984* to extend from 21 days to 90 days the maximum period during which a warrant issued under that Act for the use of a listening device remains in force if the warrant is issued in connection with certain Commonwealth terrorism offences, and the State terrorism offence

- the *Crimes Act 1900* to create a State offence that is equivalent to the Commonwealth offence of membership of a terrorist organisation.

COMMENCEMENT DATE

Assented to on 27June 2005 and commenced on 13 September 2005.

AUTHORISATION

- The Commissioner of Police may authorise an eligible police officer or the Crime Commissioner may authorise an eligible staff member of the Crime Commission to apply for a covert search warrant under this Part (s. 27D). The Commissioner of Police may delegate his power to give this authorisation to an Assistant Commissioner holding a position that is prescribed by the regulations or a person of or above the rank of superintendent that is prescribed by the regulations. No more than 2 persons may hold delegations under this section at any one time (s. 27E). Regulations (the *Terrorism (Police Powers) Regulation 2005*) have been proclaimed and are applicable here.
- Warrants may be issued only when there is a reasonable suspicion or belief that a terrorist act has been, is being, or is likely to be committed, and that the entry to and search of premises will substantially assist in responding to or preventing the terrorist act, and that it is necessary for the entry and search of those premises to be conducted without the knowledge of any occupier of the premises (s. 27C).
- Covert search warrants are issued by 'eligible judges' (s. 27K).
- If an application for a covert warrant has been refused, a further application may not be made for the same warrant unless the further application provides additional information that justifies the making of a further application. This is the same safeguard that applies to normal search warrants to discourage judge shopping (s. 27M).

LIMITATIONS

- A warrant must be executed within 30 days of issue (s. 27N(f)).

ACCOUNTABILITY

- An eligible judge who determines an application for a covert search warrant must cause a record to be made of all relevant particulars of the grounds that he/she has relied on to justify the issue of the warrant or the refusal to issue the warrant (s. 27L). Regulations (the Terrorism (Police Powers) Regulation 2005) have been proclaimed and are applicable here.
- A person to whom a covert search warrant has been issued must report back to the eligible judge who issued the warrant about the execution of the warrant within ten days after it was executed or within ten days after it expired (s. 27S).
- A person who executes a covert search warrant is to prepare an occupier's notice setting out certain details regarding the execution of the warrant. An occupier's notice must be provided for the approval of an eligible judge within six months of the execution of a covert search warrant. An eligible judge can postpone the giving of an occupier's notice for a period of up to six months at a time, for a total period of not more than 18 months. Where the execution of the search warrant involved entry to adjoining premises, similar notices are to be prepared and given to occupiers of these adjoining premises (ss. 27U and 27V).
- Annual reports must be made to the Attorney General and the Minister for Police regarding the exercise of these powers (s. 27ZB).
- The scheme is subject to independent monitoring by the NSW Ombudsman for a period of two years (s. 27ZC).[44]
- A new offence for a person to give false or misleading information to an eligible judge in an application for a covert search warrant has been created (s. 27Z). It is also an offence, with certain exceptions and in certain circumstances) for a person to intentionally or recklessly publish an application for a covert search warrant or related information (s. 27ZA).

ISSUES RAISED IN SECOND READING SPEECH & ASSOCIATED PARLIAMENTARY DEBATES[45]

When introducing the Bill, Mr Bob Debus, Attorney General and Minister for the Environment, described the powers as extraordinary and identified the need for safeguards:

[44] A minor amendment was made to Section 27ZC by the *Statue Law (Miscellaneous Provision) Act 2006* in July 2006. This amendment involved enabling this report to be included with the one prepared by the Ombudsman (under Section 26ZO) concerning preventative detention, 'so long as the requirements of this section are complied with in relation to the report prepared under this section'.

[45] NSW Legislative Assembly Hansard, 9 June 2005 and 10 June 2005; NSW Legislative Council Hansard, 22 June 2005.

> The citizens of this State have a right to expect that their privacy will be protected from unjustified searches and interference from the State. Society recognises, however, that there are certain circumstances when an individual's right to privacy must be weighed against the greater public interest in order to allow law enforcement agencies to uphold the law and prevent criminal activity, especially when many lives are potentially at stake. … The threat posed by terrorism clearly poses unique challenges. …
>
> These powers are extraordinary and will be permitted only with the strictest safeguards, including the following. Warrants may be issued only when there is a reasonable suspicion or belief that a terrorist act has been, is being, or is likely to be committed. Annual reports must be made to the Attorney General and the Minister for Police regarding the exercise of these powers. Any complaint regarding the exercise of these powers can be investigated by the established bodies, the NSW Ombudsman, the Commissioner of Police and, where appropriate, the Police Integrity Commission. The scheme will be kept under constant legislative review through the existing review provisions of the Terrorism (Police Powers) Act, which requires yearly reports. The scheme is subject to independent monitoring by the Ombudsman for a period of two years.
>
> These safeguards are an attempt to balance the legitimate needs of law enforcement and the rights of privacy that all citizens enjoy. The House will also note that schedule 4 to the bill creates an offence of membership of a terrorist organisation – under section 310J of the Crimes Act 1900. This offence is in the same terms as the membership offence under the Commonwealth legislation. … The Government considers that this provision is necessary as a temporary measure because membership of a terrorist organisation is not an offence known to New South Wales law, and New South Wales is constitutionally prevented from enacting a covert search warrant scheme for the investigation of Commonwealth terrorism offences (NSW Legislative Assembly Hansard, 9 June 2005).

Mr Bob Debus also made it clear that these powers were not intended to be used in general policing:

> The powers in this bill are not intended or designed to be used for general policing. Their use is restricted to the NSW Police Counter-Terrorism Co-ordination Command and to the units of the NSW Crime Commission assigned the task of investigating and responding to terrorism

and that counter-terrorism policing requires different tools:

> This scheme provides police with another tool that answers some of the more difficult characteristics of terrorist activity. For example, while both terrorists and organised crime gangs operate secretively and are aware of the possibility of official surveillance, terrorists operate over a much longer time frame. … So the first requirement of counter-terrorism covert investigative powers is that they be able to operate over a long period, enabling investigators to target terrorists from the early stages of their activities.
>
> Covertness is the second requirement. … This scheme will allow police to enter private premises without the knowledge of the occupiers for the purpose of preventing or responding to terrorist threats.

> The Government sees this legislation not only as an investigative tool but also as a preventative tool (NSW Legislative Assembly Hansard, 9 June 2005).

In response to debate on this legislation, Mr Bob Debus emphasised the safeguards incorporated in the legislation:

> I emphasise in this context that these powers have nothing to do with secret policing. Secret policing involves the exercise of powers by police without independent oversight, without accountability. Those sorts of powers might involve the surveillance of law-abiding members of the community who are considered suspect in some way due to their social or political leanings. The term 'secret policing' evokes the fear of the knock on the door in the middle of the night that has been known in totalitarian societies like Hitler's Germany or Stalin's Soviet Union. These powers are not secret policing powers. The Government has gone to great lengths to ensure that the bill contains strong and robust safeguards in relation to the granting of these covert search warrants and their execution, and in the requirement that an occupier must ultimately be notified that a search has taken place (NSW Legislative Assembly Hansard, 10 June 2005).

When the legislation was being debated in the Legislative Council, Ms Lee Rhiannon of the Greens raised the following concerns issues that had arisen when a Commonwealth agency had executed a search warrant:

> Let us consider the recent work of the Australian Security Intelligence Organisation (ASIO), to some extent New South Wales Federal counterpart. Mr Stephen Hopper, the previous lawyer for Mamdouh Habib, recalled that in 2001 ASIO … raided a house without a warrant because it got the address wrong, in keystone cops style confusing the house with another one down the street; and, to add insult to injury, allowed $7,000 to disappear from one house in the process. The complaint that followed has still not been dealt with and the money remains missing (NSW Legislative Council Hansard, 22 June 2005).

ISSUES RAISED BY LEGISLATIVE REVIEW COMMITTEE[46]

The Legislation Review Committee raised a number of concerns about trespasses on personal rights and liberties (pp. 38-39), exposure of persons not connected to terrorist acts (pp. 41-42) as well as risks associated with power to enter premises when occupants present (p. 42). In summary the Committee noted that:

- the broad covert search powers significantly trespass on the personal right to privacy
- the purpose of these powers is to prevent terrorist activity
- the Bill provides for significant trespasses on the rights and liberties of persons who are not suspected of being involved in the commission of a terrorist act

46 Parliament of New South Wales Legislation Review Committee (2005) *Legislation Review Digest No 8 of 2005*, 20 June 2005, pp. 33-45.

- occupants of premises who are subject to the full search and seizure powers of a warrant are not normally provided with an occupiers notice if they were not at the time believed to be knowingly concerned with the commission of the terrorist act

- the Bill provides no protection in relation to reasonable responses by occupiers discovering covert intruders who are executing a warrant (p. 42).

A3.5: TERRORISM (POLICE POWERS) AMENDMENT (PREVENTATIVE DETENTION) ACT 2005

OBJECT

To amend the *Terrorism (Police Powers) Act 2002* to allow a person to be taken into custody and detained for a short period of time in order to:

a. prevent an imminent terrorist act, or

b. preserve evidence of, or relating to, a recent terrorist act.

This is to give effect in NSW to the decision of 27 September 2005 of the Council of Australian Governments that States and Territories introduce legislation on preventative detention of persons for up to 14 days to prevent terrorist acts or preserve evidence following a terrorist act (to complement Commonwealth legislation for preventative detention for up to 48 hours). The Commonwealth legislation is an amendment to the Commonwealth Criminal Code set out in the Commonwealth *Anti-Terrorism Bill 2005*.

COMMENCEMENT DATE

Assented to on 7 December 2005 and commenced on 16 December 2005.

AUTHORISATION

- A police officer who seeks to apply for a preventative detention order must first obtain the approval of one of: the Commissioner of Police, a Deputy Commissioner of Police, or an Assistant Commissioner of Police responsible for counter-terrorism operations (s. 26F (1)).
- An application for a preventative detention order must be in writing and sworn (s. 26G (1)(a)), set out the facts and other grounds on which the police officer considers the order should be made (s. 26G (1)(b)) and specify the period for which the person is to be detained under the order (s. 26G (1)(c)). The application must also fully disclose all relevant matters of which the applicant is aware, both favourable and adverse to the making of the order (s. 26G (1)).[47]
- Orders can only be made by the Supreme Court (ss. 26H, 26I).
- The Commissioner or a Deputy Commissioner of Police, or an Assistant Commissioner of Police responsible for counter-terrorism operations, must nominate a police officer of or above the rank of superintendent to oversee the exercise of functions under or in relation to this order (s. 26R (1)) The nominated senior police officer must be someone who is not involved in the making of the application for the preventative detention order (s.26R (2)).

[47] NB An application for an interim preventative detention order can be made by telephone, fax, email or other electronic communication (s. 26G (2)) Such an interim order expires after 48 hours (s. 26L).

LIMITATIONS

- Where a preventative detention order is made to assist in preventing a terrorist attack from occurring, such a terrorist attack must be imminent and, in any event, be expected to occur at some time in the next 14 days (s. 26D (1)).
- A preventative detention order cannot be applied for or made in relation to a person who is under 16 years of age (s. 26E (1)).
- The maximum period for which a person may be detained under a preventative detention order is 14 days. That maximum period is reduced by any period of actual detention under a related order against the person in relation to the same terrorist act (s. 26K (2)). The maximum period for an interim preventative detention order is 48 hours (s. 26L).
- A police officer is not authorised to search for evidence of, or relating to, a terrorist act, unless the police officer has reasonable cause to suspect the person is carrying such evidence (s. 26V (3)).
- A person being detained cannot be questioned by a police officer except for the purpose of establishing identity or ensuring his or her safety and well being (s. 26ZK). This Act does not exclude the person being detained being questioned by someone who is not a police officer.
- A sunset provision is included so that the scheme will expire in 10 years time (s. 26ZS).

ACCOUNTABILITY

- The detained person is to be given a copy of the order and a summary of the grounds on which the order is made (s. 26ZB).
- The person being detained is entitled to contact the Ombudsman and the Police Integrity Commission (s. 26ZF). However, it is not clear that a person being detained must be informed of this entitlement to contact the Police Integrity Commission.
- The Commissioner of Police must report annually to the Attorney General and the Minister for Police on the exercise of powers under this Part by police officers. The report is to be provided within 4 months after each 30 June (s. 26ZN (1)). Specific requirements are provided for the information to be included in such reports (s. 26ZN (2)). These reports are to be tabled by the Attorney General in each House of Parliament as soon as practicable after they are received by the Attorney General (s. 26ZN (3)).
- The scheme will be monitored by the Ombudsman for a period of five years, with an interim report after two years (s. 26ZO). [48]
- The Commissioner of Police is to ensure that the Ombudsman is duly notified of the making of a preventative detention order, is duly notified if a

[48] A minor amendment was made to Section 26ZO by the *Statue Law (Miscellaneous Provision) Act 2006* in July 2006. This amendment involved enabling this report to be included with the one prepared by the Ombudsman (under Section 27ZC) concerning covert search warrants, 'so long as the requirements of this section are complied with in relation to the report prepared under this section'.

person is taken into custody under a preventative detention order, and is duly notified of the revocation of such an order (s. 26ZO (3)).

ISSUES RAISED IN SECOND READING SPEECH & ASSOCIATED PARLIAMENTARY DEBATES[49]

In introducing this legislation, Mr Milton Orkopoulos (Minister for Aboriginal Affairs and Minister Assisting the Premier on Citizenship) on behalf of Mr Debus (Attorney General and Minister for the Environment) stated that:

> This scheme implements the agreement reached at the Council of Australian Governments (COAG) meeting of 27 September 2005 and will complement the preventative detention scheme introduced by the Commonwealth Government in the Anti-Terrorism Bill (No. 2) 2005. All States and Territories of Australia agreed to enact preventative detention legislation.
>
> The New South Wales scheme replicates the Commonwealth provisions in that it provides for the detention of a person, thus incapacitating them; restrictions on communications, which is true of all arrested and detained persons; and the monitoring of the detained person's communications to ensure that there is no exchange of information between suspects or plans made to evade capture or destroy evidence. However, this bill differs in a number of important respects, namely, due to constitutional reasons the Commonwealth scheme can operate for only 48 hours. The New South Wales scheme operates for up to 14 days. The Commonwealth scheme is administrative. Initial orders are made by a senior police officer, which are later confirmed by judicial officers acting in their personal capacity.
>
> The New South Wales scheme is judicial. Both the initial and final preventative detention orders are made only by judges of the New South Wales Supreme Court. The Commonwealth scheme at no time allows a hearing on the merits between the parties before the expiry of the detention. The New South Wales scheme permits an initial preventative order to be made in the absence of the subject person. However, at subsequent confirmation or revocation hearings the detained person will be permitted to be present and to contest the matter (NSW Legislative Assembly Hansard, 17 November 2005).

ISSUES RAISED BY LEGISLATIVE REVIEW COMMITTEE[50]

The Legislation Review Committee raised a number of concerns about trespasses on personal rights and liberties.

The Committee noted that the making of an interim or final preventative detention order is based on the Court being satisfied that police have 'reasonable grounds to suspect' that the specified conditions in the section exist. 'Reasonable suspicion' and 'reasonable belief' are different standards. Requiring only suspicion on the part of the police officer applying for an interim or final preventative detention order widens the scope of these orders considerably (pp. 23-24).

---

[49] NSW Legislative Assembly Hansard 17 November 2005; NSW Legislative Council Hansard 30 November 2005.

[50] Parliament of New South Wales Legislation Review Committee (2005) Legislation Review Digest No 15 of 2005, 29 November 2005, pp. 20-39.

The Committee noted that judicial oversight of the preventative detention regime in this Bill is an important safeguard (p. 25). It raised the view that, 'without highly compelling public interest justifications, [the] maximum period is excessive and a significant trespass on what are generally considered the most fundamental human rights' (p. 25). The Committee also noted the importance of mandatory independent review for legislation that confers extraordinary powers that significantly trespass on rights in order to address specific circumstances (p. 38).

The Committee said that it considers that the acceptability of such extraordinary powers is in part dependent on:

- the duration for which the powers will exist
- the frequency of their review, and
- the level of independence of any body undertaking their review (p. 38).