Telecommunications (Interception and Access) Act 1979

Report for the year ending 30 June 2010

Produced by the Public Affairs Unit
Australian Government Attorney-General's Department
Publication number

CONTENTS

LIST OF TABLES

ABBREVIATIONS

AAT	Administrative Appeals Tribunal
ACC	Australian Crime Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
Blunn Report	Report of the *Review of the Regulation of Access to Communications*
CAC	Communications Access Co-ordinator
CCC WA	Corruption and Crime Commission of Western Australian
CMC	Queensland Crime and Misconduct Commission
Customs	Australian Customs and Border Protection Service
ICAC	Independent Commission Against Corruption (New South Wales)
NSW CC	New South Wales Crime Commission
NSW Police	New South Wales Police Force
NT Police	Northern Territory Police
OPI	Office of Police Integrity (Victoria)
PIC	Police Integrity Commission (New South Wales)
Qld Police	Queensland Police Service
SA Police	South Australia Police
Tas Police	Tasmania Police
Vic Police	Victoria Police
WA Police	Western Australia Police
2008 Amendment Act	*Telecommunications Interception Legislation Amendment Act 2008*
The TIA Act	*Telecommunications (Interception and Access) Act 1979*
Telecommunications Act	*Telecommunications Act 1997*

CHAPTER 1—INTRODUCTION

1.1 This is the twenty-second Annual Report on the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). This report relates to the period from 1 July 2009 to 30 June 2010.

1.2 Chapter 2 outlines the objectives and the structure of the TIA Act.

1.3 Chapter 3 records relevant developments that have occurred during the reporting period.

1.4 Chapter 4 presents the information collected in accordance with the statutory requirements of Part 2-8 of the TIA Act, relating to the interception of telecommunications.

1.5 Chapter 5 presents the information collected in accordance with the statutory requirements of Part 3-6 of the TIA Act, relating to accessing stored communications.

1.6 Chapter 6 presents the information collected in accordance with the statutory requirements of Part 4-2 of the TIA Act, relating to accessing telecommunications data.

CHAPTER 2—OVERVIEW OF THE ACT

2.1 This chapter provides an overview of the TIA Act, including an outline of its objects and a description of the provisions that are most relevant to the contents of this report. In addition, this chapter includes an outline of the accountability provisions of the TIA Act.

Objectives of the legislation

2.2 The TIA Act has two key purposes. Its primary objective is to protect the privacy of individuals who use the Australian telecommunications system. The TIA Act makes it an offence to intercept communications, or access stored communications, other than in accordance with the provisions of the TIA Act. The second purpose of the TIA Act is to specify the circumstances in which it is lawful to intercept, access communications or authorise the disclosure of telecommunications data.

2.3 A telecommunications service may be intercepted under the authority of a telecommunications interception warrant by an *interception agency* for the investigation of a serious offence, or by the Australian Security Intelligence Organisation (ASIO) for national security purposes. A stored communication may be covertly accessed under the authority of a stored communications warrant by an *enforcement agency* for the investigation of a serious contravention or by ASIO for national security purposes. Telecommunications data may be disclosed by a telecommunications service provider under the authorisation of an officer holding a management office or position of an *enforcement agency* for the enforcement of the criminal law or the enforcement of a law imposing a pecuniary penalty or protection of the public revenue.

Provisions relevant to this report

2.4 The foundations of the TIA Act are contained in subsections 7(1) and 108(1) which prohibit the interception of a communication passing over the telecommunications system or access to stored communications. Chapter 4 of the TIA Act allows the disclosure of telecommunications data which is ordinarily prohibited by the *Telecommunications Act 1997*.

2.5 Subsection 6(1) of the TIA Act defines interception as listening to or recording, by any means, a communication in its passage over a telecommunications system without the knowledge of the person making the communication.

2.6 The effect of section 6AA and paragraph 108(1)(b) of the TIA Act is that accessing a stored communication comprises listening to, reading or recording a stored communication where that action is done with the assistance of a carrier. The access must be without the knowledge of either the sender or the intended recipient of the communication for it to fall within the parameters of the TIA Act.

2.7 Telecommunications data is not defined in the TIA Act. Section 172 excludes the content or substance of a call from being 'telecommunications data'. Accordingly, telecommunications data could include the date, time, subscriber and location of a call.

2.8 There are exceptions to these prohibitions, the most relevant of which relate to the interception of communications, access to stored communications under a warrant or the disclosure of telecommunications data under an authorisation.

2.9 The TIA Act regulates the

- issue and revocation of warrants and authorisations
- scope of the authority conferred by warrants or authorisations
- execution of warrants, and
- use of information obtained under warrants or authorisations.

Telecommunications interception warrants

Offences for which telecommunications interception warrants may be obtained

2.10 Part 2-5 of the TIA Act provides for the issue of telecommunications interception warrants to interception agencies. This Part of the TIA Act provides that a telecommunications interception warrant can be sought to assist with the investigation of a serious offence.

2.11 A serious offence is exhaustively defined in section 5D which includes the following types of offences:

- murder, kidnapping and equivalent offences
- an offence against Division 307 of the *Criminal Code*, being serious drug import and export offences
- an offence constituted by conduct involving an act or acts of terrorism
- an offence against Subdivision A of Divisions 72, 101, 102 and 103 of the *Criminal Code*
- offences in relation to which the Australian Crime Commission (ACC) is conducting a special investigation within the meaning of the *Australian Crime Commission Act 2002*[1]
- specified offences involving particular conduct such as loss of a person's life, serious personal injury, serious damage to property in circumstances endangering personal safety, serious arson, trafficking in prescribed substances, serious fraud, serious loss to the revenue of the Commonwealth, a State or the Australian Capital Territory, or bribery or corruption of, or by, an officer of the Commonwealth or the State, where the offence is punishable by at least seven years imprisonment
- specified offences involving planning and organisation which involve conduct such as theft, handling of stolen goods, tax evasion, currency violations, bribery or corruption company violations, harbouring criminals, dealing in firearms or armaments, a sexual offence against a person who is under 16 or an immigration offence, where the offence is punishable by at least seven years imprisonment

[1] This section applies only to warrants sought by the ACC.

- offences relating to people smuggling, slavery sexual servitude, deceptive recruiting and trafficking in persons
- sexual offences against children and offences involving child pornography
- money laundering offences
- cybercrime offences
- serious drug offences
- serious cartel offences
- offences relating to criminal associations and organisations, such as associating with a criminal organisation or a member of a criminal organisation, contribute to the activities of a criminal organisation, and
- ancillary offences, such as aiding, abetting and conspiring to commit serious offences.

2.12 It is a general requirement that the offence be punishable by imprisonment for life or for a maximum period of at least seven years. However, there are exceptions to this rule. These exceptions generally apply to offences that by their nature require interception as an investigative tool or where the conduct is serious enough to warrant the use of interception regardless of the offence threshold. Examples of these types of offences include child pornography and cybercrime offences.

Applying for telecommunications interception warrants

2.13 Applications for telecommunications interception warrants may only be made by an interception agency. An interception agency is the ACC, the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Federal Police (AFP) or an 'eligible authority' of a State or the Northern Territory which is the subject of a declaration under section 34 of the TIA Act.

2.14 In effect, a section 34 declaration, which can only be made by the Attorney-General, grants interception agency status to an eligible authority. This means that the agency can then apply for telecommunications interception warrants to assist in their investigations of serious offences. An eligible authority which is *not* the subject of a declaration is *not* able to apply for such a warrant but is able to receive intercepted information for permitted purposes from an interception agency.

2.15 The TIA Act defines eligible authorities to be the police force of each of the States and of the Northern Territory. During the reporting period, 'eligible authority' was defined as:

- in New South Wales – the NSW Crime Commission, the Independent Commission Against Corruption (ICAC), the Inspector of the ICAC, the Police Integrity Commission (PIC) and the Inspector of the PIC
- in Victoria – the Office of Police Integrity (OPI)
- in Queensland – the Crime and Misconduct Commission (CMC)

- in Western Australia – the Corruption and Crime Commission of Western Australia (CCC WA) and the Parliamentary Inspector of the CCC WA.

2.16 During the reporting period, the following eligible authorities were the subject of a declaration pursuant to section 34 of the TIA Act and therefore were able to apply for telecommunications interception warrants:

AGENCY	DATE OF SECTION 34 DECLARATION
Victoria Police	28 October 1988
New South Wales Crime Commission	30 January 1989
New South Wales Police Force	30 January 1989
Independent Commission Against Corruption	6 June 1990
South Australia Police	10 July 1991
Western Australia Police	15 July 1997
Police Integrity Commission	14 July 1998
Corruption and Crime Commission of Western Australia	24 March 2004
Tasmania Police	5 February 2005
Northern Territory Police	25 October 2006
Office of Police Integrity Victoria	18 December 2006
Queensland Police Service	8 July 2009
Queensland Crime and Misconduct Commission	8 July 2009

Eligible Judges and nominated AAT members

2.17 Part 2-5 of the TIA Act provides that an eligible Judge or nominated Administrative Appeals Tribunal (AAT) member may issue a telecommunications interception warrant on application by an agency.

2.18 An 'eligible Judge' refers to a Judge of a court created by the Parliament who has consented in writing and been declared by the Attorney-General to be an eligible Judge. In the reporting period, eligible Judges were members of the Federal Court of Australia, the Family Court of Australia and the Federal Magistrates Court.

2.19 A 'nominated AAT member' refers to a Deputy President, senior member or a member of the AAT who has been nominated by the Attorney-General to issue warrants. In the case of part-time senior members and members of the AAT, the member must have been enrolled as a legal practitioner of the High Court, the Federal Court or the Supreme Court of a State or Territory for no less than five years to be eligible for nomination to issue warrants.

Form of applications

2.20 The TIA Act requires that an application for a telecommunications interception warrant be in writing and be accompanied by a supporting affidavit. However, in urgent

circumstances, applications may be made by telephone. In either case, the warrant takes effect only when completed and signed by the Judge or nominated AAT member.

2.21 The information required for a written application must also be verbally provided to a Judge or nominated AAT member at the time of a telephone application and subsequently provided in writing (within one day). Specific provision is made for the revocation of a warrant obtained by telephone where this condition is not complied with.

2.22 The TIA Act requires that an application contain the name of the agency and person making the application. The supporting affidavit must contain the facts on which the application is based, the period for which the warrant is sought to be in force and information regarding any previous warrants obtained in relation to the same matter.

Matters to be considered by an issuing authority

2.23 An issuing authority must consider the following matters before issuing a telecommunications interception warrant:

- privacy of any person or persons would be likely to be interfered with
- gravity of the offence
- how much the information likely to be obtained would assist the investigation
- the availability of alternative methods of investigation
- how much the use of the methods would assist the investigation, and
- how much the use of such methods would prejudice the investigation by the agency, whether because of delay or for any other reason.

2.24 Where an application for a warrant includes a request that the warrant authorise entry onto premises, section 48 requires that the Judge or nominated AAT member also be satisfied that it would be impracticable or inappropriate to intercept communications by less intrusive means.

Safeguards and controls relating to the telecommunications interception regime

2.25 The TIA Act contains a number of safeguards and controls in relation to interception as well as a number of reporting requirements. These requirements are designed to ensure that appropriate levels of accountability exist. The most significant of these requirements are outlined below.

Attorney-General to be given copies of telecommunications interception warrants and revocations and reports on outcomes

2.26 Sections 57, 59A and 94 of the TIA Act provides that the chief officer of each interception agency must give to the Attorney-General:

- a copy of each telecommunications interception warrant issued to that agency
- each instrument revoking such a warrant, and
- within three months of a warrant ceasing to be in force, a written report about the use made of information obtained by interception under the warrant.

Reports by carrier

2.27 Section 97 of the TIA Act provides that the Managing Director of a carrier who enables interception to occur under a warrant must report to the Attorney-General within three months of the warrant ceasing to be in force. The report must include details of the acts done by employees of the carrier to effect interception under the warrant and to discontinue interception when the warrant expires or is revoked.

General Register of telecommunications interception warrants

2.28 Section 81A of the TIA Act provides that the Secretary of the Attorney-General's Department must maintain a General Register which includes particulars of all telecommunications interception warrants. The particulars required to be recorded in the General Register are:

- the date of issue and period for which the warrant was to be in force
- the agency to which the warrant was issued and the Judge or nominated AAT member who issued the warrant
- the telecommunications service to which the warrant relates
- the name of the person specified in the warrant as the person using or likely to use the telecommunications service
- each serious offence in relation to which the Judge or nominated AAT member who issued the warrant was satisfied on the application for the warrant, and
- for named person warrants, the name of the person to whom the warrant relates and each telecommunications service that is specified in the warrant, or in relation to which interceptions authorised by the warrant have occurred.

2.29 Section 81B of the TIA Act provides that the Secretary of the Attorney-General's Department must deliver the General Register to the Attorney-General for inspection every three months. Interception agencies are notified once the Attorney-General has inspected the General Register to enable the destruction of restricted records.

Special Register of telecommunications interception warrants

2.30 Section 81C of the TIA Act provides that the Secretary of the Attorney-General's Department must maintain a Special Register recording the details of telecommunications interception warrants which did not lead, directly or indirectly, to a prosecution within three months of the expiry of the warrant. The Secretary must deliver the Special Register to the Attorney-General for inspection every three months together with the General Register.

Destruction of records

2.31 Section 79 of the TIA Act provides that agencies must destroy restricted records which are original records. Once the chief officer of the agency is satisfied that the record will not be needed for permitted purposes and the Attorney-General has inspected the relevant Register, those records must be destroyed.

Inspections

2.32 The ACC, ACLEI and the AFP are required to maintain records relating to interceptions and the use, dissemination and destruction of intercepted information. These records must be inspected by the Commonwealth Ombudsman on a regular basis.

2.33 The TIA Act requires the Commonwealth Ombudsman to report to the Attorney-General regarding these inspections and to include in his or her report a summary of any deficiencies identified and any remedial action taken.

2.34 Parallel requirements are imposed by State and Territory legislation on State and Territory interception agencies. The imposition of parallel record keeping and reporting requirements with the Commonwealth legislation is a precondition to the State or Territory eligible authority being granted interception agency status. If the Attorney-General is satisfied that the State or Territory legislation is no longer parallel to the Commonwealth legislation, he or she may revoke their interception agency status.

2.35 While the Commonwealth Ombudsman is responsible for inspecting the records of the ACC, ACLEI and the AFP, the relevant State or Territory Ombudsman generally undertakes this function for State and Territory agencies.[2] The reports of the inspections of the declared State and Territory agencies are given to the responsible State or Territory Minister who must provide a copy to the Commonwealth Attorney-General.

2.36 Accordingly, all law enforcement agencies capable of applying for telecommunications interception warrants operate under equivalent supervisory and accountability provisions. This means that the TIA Act imposes a national scheme in relation to telecommunications interception and ensures that the Attorney-General is kept informed of the agencies' activities by means of reports from the agencies and the Ombudsman.

Annual Report tabled by Attorney-General

2.37 Sections 99 and 104 of the TIA Act provide that the Attorney-General must prepare and table in Parliament each year a report setting out the information specified in Part 2-8 of the TIA Act. Chapter 4 of this report presents the required information.

[2] Instead of the State Ombudsman, inspection of the SA Police is undertaken by the Police Complaints Authority (South Australia), inspections of the Vic Police and the OPI are undertaken by the Special Investigations Monitor (Victoria), and inspections of the CMC and Qld Police are undertaken by the Public Interest Monitor (Queensland).

Stored communications warrants

Offences for which stored communications warrants may be obtained

2.38 Part 3-3 of the TIA Act enables an issuing authority to issue a stored communications warrant to an enforcement agency. The definition of enforcement agency includes listed criminal law enforcement agencies as well as agencies responsible for administering a law imposing a pecuniary penalty or relating to the protection of the public revenue. Enforcement agencies will include all the defined interception agencies plus other regulatory bodies such as the Australian Customs and Border Protection Service and the Australian Securities and Investments Commission.

Applying for a stored communications warrant

2.39 A stored communications warrant authorises covert access to stored communications in connection with the investigation of a serious contravention. A 'serious contravention' is defined by the TIA Act as a:

- serious offence (being an offence for which a telecommunications interception warrant may be obtained)
- an offence punishable by a maximum period of imprisonment of at least three years imprisonment, or
- an offence with an equivalent monetary penalty.

Issuing authorities

2.40 Part 3-3 of the TIA Act provides that an enforcement agency may apply to an issuing authority for a stored communications warrant to access stored communications. Section 6DB of the TIA Act provides that the Attorney-General may appoint issuing authorities to issue stored communications warrants.

2.41 Paragraph 6DB(1)(a) defines an issuing authority as a Judge of a court created by the Parliament, a Federal Magistrate or a State magistrate, who has consented in writing to being appointed by the Attorney-General and who has been so appointed by the Attorney-General. In the reporting period, issuing authorities included members of the Federal Court of Australia, the Family Court of Australia, the Federal Magistrates Court and State magistrates. It should be noted that appointed State magistrates, while able to issue stored communications warrants, are not able to be declared to be able to issue telecommunications interception warrants.

2.42 Paragraph 6DB(1)(b) further defines an issuing authority as including a person who is a Deputy President, senior member or a member of the AAT and has been appointed as an issuing authority by the Attorney-General. The member must have been enrolled as a legal practitioner of a Federal Court or of the Supreme Court of a State or a Territory for at least five years before they are eligible to be appointed as an issuing authority.

Form of applications

2.43 In the normal course of events, the TIA Act requires that an application for a stored communications warrant be in writing and accompanied by a supporting affidavit. However, in urgent circumstances, applications may be made by telephone. In either case, the warrant takes effect only when completed and signed by the issuing authority.

2.44 The information required for a written application must also be verbally provided to a Judge or nominated AAT member at the time of a telephone application and subsequently provided in writing (within one day). Specific provision is made for the revocation of a warrant obtained by telephone where this condition is not complied with.

2.45 The TIA Act requires that an application contain the name of the agency and person making the application. The supporting affidavit must contain the facts on which the application is based.

Matters to be considered by an issuing authority

2.46 An issuing authority must consider the following matters before issuing a stored communications warrant:

- privacy of any person or persons would be likely to be interfered with
- the gravity of the conduct constituting the serious contravention
- how much information would be likely to assist the investigation
- the availability of alternative investigative methods
- how much the use of such methods would assist the investigation, and
- how much the use of such methods would prejudice the investigation by the agency, whether because of delay or for any other reason

Safeguards and controls relating to the stored communications regime

2.47 The TIA Act contains a number of safeguards and controls in relation to stored communications warrants as well as a number of reporting requirements. These requirements are designed to ensure that appropriate levels of accountability exist.

Recordkeeping

2.48 Section 151 of the TIA Act provides that the chief officer of an enforcement agency must cause to be kept:

- each stored communications warrant issued
- each instrument of revocation

- copies of authorisations which authorise persons to receive stored communications and

- particulars of the destruction of information.

Destruction of records

2.49 Section 150 of the TIA Act provides that if the chief officer of an agency is satisfied that the information or record obtained by accessing a stored communication is not likely to be required for the purposes for which it can be used under the TIA Act, that information or record must be destroyed.

Inspections

2.50 The TIA Act provides that the Commonwealth Ombudsman may conduct regular inspections of records and must report to the Attorney-General on the results of those inspections.

Annual report tabled by Attorney-General

2.51 Sections 161 and 164 of the TIA Act provide that the Attorney-General must prepare and table in Parliament each year a report setting out the information specified in Part 3-6 of the TIA Act. Chapter 5 of this report presents the required information.

Telecommunications data authorisations

Telecommunications data

2.53 Part 4-1 of the TIA Act enables enforcement agencies to authorise the disclosure of telecommunications data.

2.54 Section 172 prohibits the disclosure of any content or substance of a communication. While telecommunications data is not defined in the TIA Act, it is taken to mean anything that is not the content or substance of a communication. It can include:

- subscriber information

- telephone numbers of the parties involved in the communication

- the date and time of a communication

- the duration of a communication

- Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication, and

- location-based information.

2.55 Sections 174 – 180 allow for the authorisation of the release of telecommunications data under certain circumstances.

Historical data

2.56 Historical or existing data is data which came into existence before the time the person from whom the disclosure is sought received notification of the authorisation. It does not include information which came into existence after notification was received but before the authorisation was executed.

2.57 The disclosure of historical or existing data may be authorised by an enforcement agency when it is considered reasonably necessary, by an authorising officer, for the enforcement of a criminal law or a law imposing a pecuniary penalty or for the protection of the public revenue.

Prospective data

2.58 Prospective data is data that comes into existence during the period for which the authorisation is in force. It does not include data that came into existence before the authorisation was in force.

2.59 The disclosure of prospective data may be authorised by a criminal law-enforcement agency when it is considered reasonably necessary, by an authorising officer, for the investigation of an offence with a maximum prison term of at least three years.

2.60 An authorisation for the disclosure of prospective data comes into force at the time the person from whom the disclosure is sought receives notification of the authorisation. The authorisation must end at a specified time no longer than 45 days from the day the authorisation is made, unless it is revoked earlier.

Who may authorise historical and prospective telecommunications data authorisations

2.61 A historical data authorisation may only be authorised by an authorised officer of the enforcement agency. A prospective data authorisation may only be authorised by an authorised officer of the criminal law-enforcement agency. An authorised officer includes:

- the head (however described) or a person acting as that head
- deputy head (however described) or a person acting as that deputy head, or
- a person who holds or is acting in an office or position covered by an authorisation in force under subsection 5AB(1) of the TIA Act.

Forms of application

2.62 Section 183 of the TIA Act provides that an authorisation under Division 3 or 4 of Part 4-1, a notification, revocation or notification of revocation must be in written or electronic form and must comply with any requirements put in place by the Communications Access Co-ordinator (CAC). The requirements for an authorisation include:

- the identity of the agency
- the basis on which the agency is an enforcement agency or criminal law-enforcement agency
- the identity of the authorised officer who is making the authorisation
- the basis on which the authorised officer is an authorised officer
- the relevant provisions of the TIA Act
- the name of the person from whom the disclosure is sought
- details of the information or documents to be disclosed
- for access to existing information or documents, a statement that the authorised officer is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty or the protection of the public revenue
- for access to prospective information or documents, a statement that the authorised officer is satisfied that the disclosure is reasonably necessary for the investigation of an offence punishable by imprisonment for at least three years
- for access to prospective information or documents, a statement that the authorised officer has had regard to how much the privacy of any person or persons would be likely to be interfered with and that the authorised officer is satisfied that the impact on privacy is outweighed by the seriousness of the conduct being investigated, and
- the date on which the authorisation is made, and for access to prospective information or documents, the date on which the authorisation is to end.

2.63 Section 184 requires a relevant staff member from an agency making an authorisation to notify the person from whom the disclosure is sought.

Safeguards and controls relating to the telecommunications data regime

Recordkeeping and inspections

2.64 Section 185 of the TIA Act provides that the head of an enforcement agency must retain an authorisation made for three years beginning on the day the authorisation is made.

Annual report tabled by Attorney-General

2.65 Section 186 of the TIA Act provides that the agencies must provide the Attorney-General statistics about the number of authorisations made under sections 178, 179 and 180. Section 186 also provides that the Attorney-General must prepare and table in Parliament each year a report setting out this information, which is presented in Chapter 6.

CHAPTER 3—DEVELOPMENTS IN THE REPORTING PERIOD

3.1 This chapter sets out the principal legislative developments and judicial decisions affecting the TIA Act during the reporting period. It also outlines comments made by intercepting agencies in relation to the value and importance of interception under telecommunications interception warrants.

Recent legislative and policy developments

Trade Practices Amendment (Cartel Conduct and Other Measures) Act 2009

3.2 The *Trade Practices Amendment (Cartel Conduct and Other Measures) Act 2009* amended the *Trade Practices Act 1974*, the *Proceeds of Crime Act 2002,* and the *Telecommunications (Interception and Access) Act 1979* to establish criminal penalties for serious cartel conduct and enable interception to be used to investigate serious cartel offences. This could occur via joint investigations between an interception agency and the Australian Competition and Consumer Commission.

3.3 The maximum criminal penalty for serious cartel conduct for an individual is 10 years imprisonment and/or a fine of $220,000. Penalties for corporations mirror the existing maximum pecuniary penalties for breaches of the civil penalty provisions, which the greater of $10 million, or three times the benefit obtained if this can be determined, or otherwise 10 per cent of annual turnover.

3.4 Telecommunication interception is an important tool for agencies when investigating serious cartel conduct.

Telecommunications (Interception and Access) Amendment Act 2010

3.5 The increased use of online services by individuals, governments, business and the not-for-profit sector means sensitive information is regularly transmitted and stored electronically. Protecting information and computer infrastructure from malicious attack is a key concern for governments and for the growing number of computer network owners whose networks hold and transmit such information.

3.6 The TIA Act previously contained special exemptions that enabled interception and security agencies, as well as certain Government Departments, to access communications on their own computer network for network protection activities. These ceased to have effect after 12 December 2009.

3.7 The *Telecommunications (Interception and Access) Amendment Act 2010* (TIA Amendment Act 2010) established a comprehensive solution covering both the public and private sectors to:

- enable all owners and operators of computer networks to undertake activities to operate, maintain and protect their networks
- enable Commonwealth agencies, security authorities and eligible State authorities to ensure that their computer network is appropriately used by employees, office holders or contractors of the agency or authority, and

- limit secondary use and disclosure of information obtained through network protection activities to:
    a) network protection purposes
    b) undertaking disciplinary action against an employee, office holder or contractor of a Commonwealth agency, security authority and eligible authority of a State who has been given access to a network, and
    c) reporting illegal behaviour that attracts a minimum of three years' imprisonment penalty threshold to the relevant authorities, and
- require the destruction of records obtained by undertaking network protection activities when the information is no longer required for those purposes.

3.8 The TIA Amendment Act 2010 also improved the effectiveness of the Australian telecommunications access regime by:

- extending the evidentiary certificate regime to lawful access to telecommunications data authorised under Chapter 4 of the TIA Act and allowing the Managing Director or the Secretary of a carrier to delegate their evidentiary certificate functions
- clarifying that lawfully intercepted information can be used, communicated and used in proceedings by the AFP in applications for interim and final control orders and initial and final preventative detention orders under Divisions 104 and 105 of the *Criminal Code Act 1995*, and
- making consequential amendments to reflect amendments to the *Police Integrity Commission Act 1996* (NSW) in relation to the investigation of the corrupt conduct of an administrative officer of the NSW Police or the misconduct of an officer of the NSW CC.

Crimes Legislation Amendment (Serious and Organised Crime) Act 2010

3.9 In April 2009, the Standing Committee of Attorneys-General (SCAG) agreed to a set of resolutions for a comprehensive national response to combat organised crime. The SCAG resolutions dealt with both the legislative and operational response to organised criminal activity.

3.10 The *Crimes Legislation Amendment (Serious and Organised Crime) Act 2010* (SOC1 Act) partially implemented the resolutions for a national response, by implementing the Commonwealth's commitment as part of the SCAG agreement to enhance its legislation to combat organised crime by:

- strengthening criminal asset confiscation, including introducing unexplained wealth provisions
- enhancing police powers to investigate organised crime by implementing model laws for controlled operations, assumed identities and witness identity protection
- addressing the joint commission of criminal offences, and
- facilitating greater access to telecommunications interception for criminal organisation offences.

3.11 Schedule 4 Part 2 of the SOC1 Act amended the definition of 'serious offence' within section 5D of the TIA Act to include particular conduct that would target associating with, contributing to, aiding and conspiring with a criminal organisation or a member of that organisation for the purpose of supporting the commission of prescribed offences.

3.12 This amendment allows telecommunications interception to be available for the investigation of these offences by State and Territory law enforcement agencies.

3.13 Schedule 4 Part 2 also included amendments to define 'associate', 'criminal organisation' and 'member'. The amendments respond to the growing effect of organised crime on the Australian community and recent legislative action from State and Territory Governments that have introduced new serious and organised crime offences.

Crimes Legislation Amendment (Serious and Organised Crime) Act (No. 2) 2010

3.14 In August 2009, SCAG agreed to further legislative and operational arrangements to support the national response to organised crime.

3.15 The *Crimes Legislation Amendment (Serious and Organised Crime) Act (No. 2) 2010* (SOC2 Act) fully implemented legislative aspects of the national response referred to at section 3.9 above. It also included additional measures to strengthen existing laws to more effectively prevent, investigate and prosecute organised crime activity, and target the proceeds of organised criminal groups.

3.16 The SOC2 Act:

- strengthened criminal asset confiscation and anti-money laundering laws
- enhanced search and seizure powers and the ability of law enforcement to access data from electronic equipment
- improved the operation of the National Witness Protection Program, including by increasing protection for current and former participants and officers involved in its operation
- introduced new offences that would target persons involved in organised crime, and facilitates greater access to telecommunications interception for the investigation of new serious and organised crime offences
- improved the operation and accountability of the ACC
- improved money laundering, bribery, and drug importation offences
- made minor and consequential amendments to correct references to provisions dealing with the extension of criminal liability, and
- made an urgent amendment to preserve the ability of federal defendants in Victoria to appeal a finding that they are unfit to plead.

3.17 Schedule 4 of the SOC2 Act inserted new offences targeting persons involved in serious and organised crime into the *Criminal Code Act 1995* (Criminal Code) and included amendments to facilitate greater access to telecommunications interception powers for the investigation of the new offences.

3.18 The amendments also introduced new offences criminalising associating with persons involved in organised criminal activity, as well as those supporting, committing crimes for or directing the activities of a criminal organisation. Schedule 4 amended the TIA Act to ensure that telecommunications interception warrants are available for the investigation of the new organised crime offences. This reflects the growing effect of organised crime on the Australian community and the need for law enforcement agencies to have access to a full suite of powers to combat such crime.

3.19 Schedule 7 of the SOC2 Act amended the *Australian Crime Commission Act 2002* (ACC Act) to improve the operation and accountability of the ACC, including enhancing the ACC's powers to deal with uncooperative witnesses, clarifying procedural powers for issuing summons and notices to produce, and requiring regular independent review of the ACC. The amendments provided the ACC with the power to refer an uncooperative witness in an examination to a superior court to be dealt with as if the witness was in contempt of that court. Part 2 of Schedule 7 of the SOC2 Act amended the TIA Act to allow lawfully intercepted information to be used in evidence in proceedings in respect of contempt of the ACC.

Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010

3.20 The sexual exploitation of children is a devastating and widespread form of criminal activity. Responsibility for combating child sexual exploitation is shared between the Commonwealth, States and Territories. Traditionally, the States and Territories have been responsible for child sex-related offences occurring domestically (eg within each jurisdiction), while the Commonwealth has enacted child sex-related offences occurring across or outside Australian jurisdictions (eg where the Internet is involved or where the offence is committed overseas). This reflects areas of Commonwealth legislative power under the Constitution.

3.21 The *Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010* (SOAC Act) amended the existing regime to ensure comprehensive coverage of sexual offences against children, and to reflect best practice approaches domestically and internationally. The legislation strengthened existing offences and introduced new offences for dealing in child pornography and child abuse material overseas and for using a postal service or similar service or carriage service for child sex-related activity.

3.22 Part 3 of Schedule 1 of the SOAC Act made minor consequential amendments to the TIA Act to ensure that the existing powers to intercept communications would extend to the new offences inserted into the Criminal Code introduced by the SOAC Act. Interception powers are now available to combat all Commonwealth child sex-related offences in the Criminal Code, whether or not the offence carries a maximum penalty of at least seven years imprisonment. This reflects the serious nature of Commonwealth child sex offences, which warrant the use of covert powers.

Anti-People Smuggling and Other Measures Act 2010

3.23 The *Anti-People Smuggling and Other Measures Act 2010* (APSOM Act) strengthened the Commonwealth's anti-people smuggling legislative framework by ensuring that an appropriate range of offences are available to target and deter people smuggling activities and create greater harmonisation across Commonwealth legislation. It put in place laws to provide greater deterrence of people smuggling activity and address the serious consequences of such activity, and provided greater capacity for Australian Government agencies to investigate and disrupt people smuggling networks.

3.24 Part 1 of Schedule 1 amended the *Migration Act 1958* and the *Criminal Code Act 1995* (the Criminal Code) to strengthen the Commonwealth legislative framework on people smuggling offences.

3.25 Part 2 of Schedule 1 amended the definition of 'serious offence' within section 5D of the TIA Act to streamline the use of telecommunications interception powers to combat people smuggling. Section 5D was also amended to include the new people smuggling offences introduced into the Migration Act and the Criminal Code to enable these offences to be investigated with the assistance of the telecommunications interception.

3.26 Schedule 3 of the APSOM Act amended the TIA Act to align the definition of foreign intelligence in the TIA Act with the concept of foreign intelligence in the *Intelligence Services Act 2001* (IS Act) which is more relevant to the current security environment.

3.27 The amendment recognises that in an increasingly interconnected global community, activities such as people smuggling are usually undertaken by non-State actors, and enables information about foreign individuals or groups operating without government support to be collected. The amendment also recognises the broader nature of the contemporary threat environment by allowing the collection of foreign intelligence about non-State actors where it is in the interests of Australia's national security, foreign relations or national economic well-being.

Previous Annual Report

3.28 The Annual Report for the year ending 30 June 2009 was tabled in the House of Representatives on 9 February 2010 and in the Senate on 23 February 2010.

Effectiveness of interception

3.29 There remains a consistent view among agencies that telecommunications interception continues to be an extremely valuable investigative tool. Agencies have again noted that evidence gathered through the execution of a telecommunications interception warrant can lead to the successful conclusion of an investigation in circumstances where alternative evidence is uncorroborated, unavailable or insubstantial.

CHAPTER 4—TELECOMMUNICATIONS INTERCEPTION INFORMATION REQUIRED UNDER THE ACT

The information required

4.1 Part 2-8 of the TIA Act provides that this report must include the following information:

- the number of applications for warrants made and the number of warrants issued (section 100)
- the duration for which warrants were specified to be in force when issued and the period for which the warrants were actually in force (section 101)
- the number of arrests, prosecutions and convictions during the reporting period based on intercepted information (section 102)
- the number of times an agency intercepted a communication without a warrant in an emergency situation such as a siege, kidnapping or extortion (section 102A)
- the total expenditure and the average expenditure per warrant incurred by relevant agencies in connection with the execution of warrants during the reporting period (paragraph 103(a))
- information about the availability of Judges to issue warrants and the extent to which nominated AAT members have been used for that purpose (paragraph 103(ab))
- the number of interceptions carried out on behalf of other agencies (paragraph 103(ac))
- the number and type of emergency service facilities that were declared by the Attorney-General for each State and Territory during the reporting period (paragraph 103(ad))
- a summary of the information required under subsection 84(1A) to be included in the report by the Ombudsman (paragraph 103(ae)), and
- additional matters (if any) as have been prescribed under the TIA Act (paragraph 103(b)). No additional matters have been prescribed for the purpose of this paragraph.

4.2 The TIA Act provides that the information must be set out in relation to each interception agency and, where relevant, each eligible authority. In addition, the information must be combined for all agencies to indicate the overall use and effectiveness of telecommunications interception under the TIA Act.

Which agencies may seek telecommunications interception warrants

4.3 During the reporting period, the following agencies were entitled to apply for telecommunications interception warrants for law enforcement purposes:

- Australian Commission for Law Enforcement Integrity
- Australian Crime Commission
- Australian Federal Police
- Corruption and Crime Commission (Western Australia)
- Crime and Misconduct Commission (Queensland)
- Independent Commission Against Corruption (New South Wales)
- New South Wales Crime Commission
- New South Wales Police Force
- Northern Territory Police
- Office of Police Integrity (Victoria)
- Police Integrity Commission (New South Wales)
- Queensland Police Service
- South Australia Police
- Tasmania Police
- Victoria Police, and
- Western Australia Police.

Applications for telecommunications interception warrants

4.4 Paragraphs 100(1)(a) and (2)(a) of the TIA Act provide that the report must set out how many applications for telecommunications interception warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting period for each agency and for all agencies in total.

4.5 During the reporting period, 3,584 warrants were issued to law enforcement agencies under Part 2-5 of the TIA Act. The total number of warrants issued increased by approximately 11% on the total number of warrants issued during the previous reporting period. Fluctuations in the number of warrants issued over the past three reporting periods are consistent with operational practices. This information is presented in Table 1.

Table 1 – Applications for telecommunications interception warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		07/08	08/09	09/10
ACC	Made Refused/withdrawn Issued	179 - 179	154 - 154	210 - 210
ACLEI	Made Refused/withdrawn Issued	- - -	- - -	1 - 1
AFP	Made Refused/withdrawn Issued	533 3 530	573 1 572	642 1 641
CCC WA	Made Refused/withdrawn Issued	102 - 102	49 - 49	40 - 40
CMC	Made Refused/withdrawn Issued	- - -	- - -	18 - 18
ICAC	Made Refused/withdrawn Issued	33 - 33	32 - 32	14 - 14
NSW CC	Made Refused/withdrawn Issued	672 - 672	622 3 619	368 1 367
NSW POLICE	Made Refused/withdrawn Issued	814 3 811	838 7 831	1142 1 1141
NT POLICE	Made Refused/withdrawn Issued	39 2 37	47 2 45	50 - 50
OPI	Made Refused/withdrawn Issued	78 - 78	65 - 65	36 - 36
PIC	Made Refused/withdrawn Issued	91 - 91	115 - 115	48 - 48
QLD POLICE	Made Refused/withdrawn Issued	- - -	- - -	173 1 172
SA POLICE	Made Refused/withdrawn Issued	124 - 124	105 - 105	113 - 113
TAS POLICE	Made Refused/withdrawn Issued	17 - 17	15 - 15	21 1 20
VIC POLICE	Made Refused/withdrawn Issued	373 - 373	331 - 331	388 - 388
WA POLICE	Made Refused/withdrawn Issued	199 - 199	287 - 287	325 - 325
TOTAL [paragraph 100(2)(a)]	**Made** **Refused/withdrawn** **Issued**	**3,254** **8** **3,246**	**3,233** **13** **3,220**	**3,589** **5** **3,584**

Telephone applications for telecommunications interception warrants

4.6 Section 40 of the TIA Act provides that an application for a telecommunications interception warrant may be made by telephone in urgent circumstances. Paragraphs 100(1)(b) and (2)(b) of the TIA Act provide that the report must set out the number of telephone applications for warrants, the number of warrants issued to each agency and the total number of warrants issued on the basis of telephone applications. The information required under paragraphs 100(1)(b) and (2)(b) is presented in Table 2.

4.7 The total number of telephone applications made in the reporting period has increased by approximately 56% on the total number of telephone applications made during the previous reporting period.

Table 2—Telephone applications for telecommunications interception warrants

AGENCY	RELEVANT STATISTICS	TELEPHONE APPLICATIONS FOR WARRANTS		
		07/08	08/09	09/10
AFP	Made	2	2	5
	Refused/withdrawn	-	-	-
	Issued	2	2	5
NSW POLICE	Made	22	22	38
	Refused/withdrawn	-	-	-
	Issued	22	22	38
TAS POLICE	Made	6	1	-
	Refused/withdrawn	-	-	-
	Issued	6	1	-
VIC POLICE	Made	27	16	23
	Refused/withdrawn	-	-	-
	Issued	27	16	23
WA POLICE	Made	-	2	1
	Refused/withdrawn	-	-	-
	Issued	-	2	1
TOTAL [paragraph 100(2)(b)]	**Made**	**57**	**43**	**67**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**57**	**43**	**67**

Renewal applications for telecommunications interception warrants

4.8 Agencies may apply for a new warrant in respect of a service or person while an existing warrant is still in force – this is known as a renewal warrant. Paragraphs 100(1)(c) and (2)(c) of the TIA Act provide that the report must set out the number of renewal applications made in relation to each agency and in total for all agencies. This information is presented in Table 3.

4.9 The number of renewal applications increased by approximately 40% in comparison with the number of renewal applications made in the previous reporting period.

Table 3— Renewal applications for telecommunications interception warrants

AGENCY	RELEVANT STATISTICS	RENEWAL APPLICATIONS		
		07/08	08/09	09/10
ACC	Made Refused/withdrawn Issued	46 - 46	37 - 37	50 - 50
AFP	Made Refused/withdrawn Issued	103 - 103	112 - 112	220 - 220
CCC WA	Made Refused/withdrawn Issued	50 - 50	12 - 12	7 - 7
CMC	Made Refused/withdrawn Issued	- - -	- - -	3 - 3
ICAC	Made Refused/withdrawn Issued	6 - 6	2 - 2	3 - 3
NSW CC	Made Refused/withdrawn Issued	111 - 111	70 - 70	42 - 42
NSW POLICE	Made Refused/withdrawn Issued	116 - 116	104 - 104	169 - 169
NT POLICE	Made Refused/withdrawn Issued	- - -	4 - 4	5 - 5
OPI	Made Refused/withdrawn Issued	23 - 23	2 - 2	11 - 11
PIC	Made Refused/withdrawn Issued	10 - 10	30 - 30	25 - 25
QLD POLICE	Made Refused/withdrawn Issued	- - -	- - -	14 - 14
SA POLICE	Made Refused/withdrawn Issued	1 - 1	3 - 3	1 - 1
TAS POLICE	Made Refused/withdrawn Issued	- - -	- - -	5 - 5
VIC POLICE	Made Refused/withdrawn Issued	56 - 56	43 - 43	56 - 56
WA POLICE	Made Refused/withdrawn Issued	29 - 29	51 - 51	45 - 45
TOTAL [paragraph 100(2)(c)]	**Made** **Refused/withdrawn** **Issued**	**551** **-** **551**	**470** **-** **470**	**656** **-** **656**

Applications for telecommunications interception warrants authorising entry onto premises

4.10 Subsection 48(1) of the TIA Act provides that an application for a telecommunications interception warrant may include a request that the warrant authorise entry onto premises. Paragraphs 100(1)(d) and (2)(d) of the TIA Act provide that the report must set out the number of applications for warrants that include requests for authorisation of entry onto premises. This information is set out in Table 4.

4.11 Agencies sought and were issued with a very small number of such warrants, which is consistent with the last three reporting periods.

Table 4—Applications for telecommunications interception warrants authorising entry on premises

AGENCY	RELEVANT STATISTICS	WARRANTS AUTHORISING ENTRY ON PREMISES		
		07/08	08/09	09/10
AFP	Made	7	7	1
	Refused/withdrawn	-	-	-
	Issued	7	7	1
CCC WA	Made	1	2	2
	Refused/withdrawn	-	-	-
	Issued	1	2	2
NSW CC	Made	-	5	-
	Refused/withdrawn	-	-	-
	Issued	-	5	-
PIC	Made	-	3	1
	Refused/withdrawn	-	-	-
	Issued	-	3	1
TOTAL [paragraph 100(2)(d)]	**Made**	**8**	**17**	**4**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**8**	**17**	**4**

Telecommunications interception warrants issued with specific conditions or restrictions

4.12 Subsection 49(1) of the TIA Act provides that a telecommunications interception warrant may specify conditions and restrictions regarding the interception of communications under that warrant. Paragraphs 100(1)(e) and (2)(e) of the TIA Act provide that the number of warrants issued with conditions and restrictions must be set out in the report. This information is set out in Table 5.

4.13 There was a significant decrease (71%) in the number of warrants issued with conditions or restrictions when compared to the previous reporting period. The ability to impose conditions or restrictions is at the discretion of the issuing authority.

Table 5—Telecommunications interception warrants issued with specific conditions or restrictions

AGENCY	WARRANTS ISSUED WITH CONDITIONS OR RESTRICTIONS		
	07/08	08/09	09/10
ACC	2	-	-
AFP	1	5	2
ICAC	-	2	-
NSW CC	26	10	-
NSW POLICE	13	4	4
PIC	3	-	1
TAS POLICE	-	3	-
TOTAL [paragraph 100(2)(e)]	**45**	**24**	**7**

Interpretative note relating to telecommunications interception warrants issued with specific conditions or restrictions

4.14 The decrease in telecommunications interception warrants issued with specific conditions or restrictions is attributable to an operational shift in obtaining warrants over mobile phones as opposed to landlines. This overcomes privacy issues which arise when a third party other than the target may be captured using a landline which is under interception.

Named person warrants

4.15 Paragraph 100(1)(ea) of the TIA Act provides that the report include the same statistics outlined above in relation to named person warrants. This means that the following statistics must be provided:

- the number of named person warrants applied for, refused and issued
- the number of telephone applications for named person warrants, made, refused and issued
- the number of renewal applications for named person warrants, made, refused and issued
- the number of named person warrants which authorise entry onto premises, and
- the number of named person warrants issued with conditions or restrictions attached.

4.16 Paragraph 100(2)(ea) of the TIA Act provides that the report must also include these statistics in total across all agencies. Tables 6 to 9 set out the information supplied by intercepting agencies regarding named person warrants. The number of named

person warrants issued to agencies increased by approximately 27% from the number of warrants issued in the previous reporting period. The number of renewal applications for named person warrants increased by approximately 25% from the previous reporting period. No named person warrants authorised entry onto premises during the reporting period.

Interpretative note relating to named person warrants

4.17 The decrease in named person warrants is attributable to operational priorities and the ability of interception agencies to obtain individual service warrants over services which a person may be using. This demonstrates the high impact on privacy that named person warrants have, and that agencies only use them when necessary and other alternative methods are not available. The named person warrant regime provides an efficient and effective method for interception agencies to be able to intercept communications by an individual as new services become known.

Table 6—Original applications for named person warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR NAMED PERSON WARRANTS		
		07/08	08/09	09/10
ACC	Made Refused/withdrawn Issued	99 - 99	103 - 103	103 - 103
AFP	Made Refused/withdrawn Issued	131 1 130	113 - 113	155 - 155
CCC WA	Made Refused/withdrawn Issued	3 - 3	2 - 2	3 - 3
CMC	Made Refused/withdrawn Issued	- - -	- - -	8 - 8
ICAC	Made Refused/withdrawn Issued	- - -	1 - 1	2 - 2
NSW POLICE	Made Refused/withdrawn Issued	41 1 40	28 - 28	25 - 25
NSW CC	Made Refused/withdrawn Issued	57 - 57	60 1 59	48 - 48
NT POLICE	Made Refused/withdrawn Issued	7 - 7	7 - 7	10 - 10
OPI	Made Refused/withdrawn Issued	10 - 10	10 - 10	- - -
PIC	Made Refused/withdrawn Issued	- - -	4 - 4	2 - 2
QLD POLICE	Made Refused/withdrawn Issued	- - -	- - -	26 - 26
SA POLICE	Made Refused/withdrawn Issued	10 - 10	6 - 6	27 - 27
TAS POLICE	Made Refused/withdrawn Issued	- - -	1 - 1	1 - 1
VIC POLICE	Made Refused/withdrawn Issued	90 - 90	66 - 66	87 - 87
WA POLICE	Made Refused/withdrawn Issued	30 - 30	33 - 33	53 - 53
TOTAL [paragraph 100(ea)]	**Made** **Refused/withdrawn** **Issued**	**478** **2** **476**	**434** **1** **433**	**550** **-** **550**

Table 7—Telephone applications for named person warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		07/08	08/09	09/10
VIC POLICE	Made Refused/withdrawn Issued	5 - 5	4 - 4	2 - 2
TOTAL [paragraph 100(ed)]	**Made** **Refused/withdrawn** **Issued**	**5** **-** **5**	**4** **-** **4**	**2** **-** **2**

Table 8—Renewal applications for named person warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		07/08	08/09	09/10
ACC	Made Refused/withdrawn Issued	40 - 40	30 - 30	36 - 36
AFP	Made Refused/withdrawn Issued	43 - 43	40 - 40	62 - 62
CCC WA	Made Refused/withdrawn Issued	- - -	- - -	1 - 1
CMC	Made Refused/withdrawn Issued	- - -	- - -	2 - 2
ICAC	Made Refused/withdrawn Issued	- - -	- - -	1 - 1
NSW CC	Made Refused/withdrawn Issued	13 - 13	14 - 14	8 - 8
NSW POLICE	Made Refused/withdrawn Issued	14 - 14	13 0 13	4 - 4
NT POLICE	Made Refused/withdrawn Issued	- - -	3 - 3	2 - 2
OPI	Made Refused/withdrawn Issued	6 - 6	- - -	1 - 1
QLD POLICE	Made Refused/withdrawn Issued	- - -	- - -	5 - 5
SA POLICE	Issued Refused/withdrawn Issued	- - -	2 - 2	1 - 1
VIC POLICE	Made Refused/withdrawn Issued	24 - 24	9 - 9	17 - 17
WA POLICE	Made Refused/withdrawn Issued	4 - 4	11 - 11	12 - 12
TOTAL [paragraph 100(ed)]	**Made** **Refused/withdrawn** **Issued**	**144** **-** **144**	**122** **-** **122**	**152** **-** **152**

Table 9—Named person warrants issued with conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR NAMED PERSON WARRANTS WITH CONDITIONS		
		07/08	08/09	09/10
ACC	Issued	1	-	-
AFP	Issued	-	1	-
NSW CC	Issued	-	1	-
TOTAL [paragraph 100(2)(ea)]	**Issued**	**1**	**2**	**-**

4.18 Paragraphs 100(1)(eb) and (2)(eb) of the TIA Act provide that the report must include, for each agency and in total, the number of named person warrants issued which involved the interception of services in the following ranges:

- the number of warrants involving interception of a single telecommunications service
- the number of warrants involving interception of between two and five telecommunications services
- the number of warrants involving interception of between six and ten telecommunications services, and
- the number of warrants involving interception of more than ten telecommunications services.

4.19 This information is included in Table 10.

Table 10—Number of services intercepted under named person warrants

AGENCY	RELEVANT STATISTICS	NUMBER OF SERVICES		
		07/08	08/09	09/10
ACC	1 service only	31	29	19
	2 – 5 services	59	66	76
	6 – 10 services	6	8	7
	10+ services	1	-	1
AFP	1 service only	27	13	31
	2 – 5 services	73	91	96
	6 – 10 services	18	10	13
	10+ services	8	2	1
CCC WA	1 service only	-	-	1
	2 – 5 services	2	2	2
	6 – 10 services	1	-	-
	10+ services	-	-	-
CMC	1 service only	-	-	3
	2 – 5 services	-	-	5
	6 – 10 services	-	-	1
	10+ services	-	-	-
ICAC	1 service only	-	-	-
	2 – 5 services	2	1	2
	6 – 10 services	-	-	-
	10+ services	-	-	-
NSW CC	1 service only	12	9	9
	2 – 5 services	34	42	27
	6 – 10 services	10	8	12
	10+ services	1	-	-
NSW POLICE	1 service only	11	6	3
	2 – 5 services	29	20	18
	6 – 10 services	-	1	2
	10+ services	-	-	-
NT POLICE	1 service only	1	1	1
	2 – 5 services	5	5	9
	6 – 10 services	1	1	-
	10+ services	-	-	-
OPI	1 service only	1	1	-
	2 – 5 services	8	8	2
	6 – 10 services	1	1	-
	10+ services	-	-	-
PIC	1 service only	-	-	-
	2 – 5 services	-	2	2
	6 – 10 services	-	2	2
	10+ services	-	-	-
QLD POLICE	1 service only	-	-	3
	2 – 5 services	-	-	23
	6 – 10 services	-	-	-
	10+ services	-	-	-
SA POLICE	1 service only	5	3	5
	2 – 5 services	4	3	19
	6 – 10 services	1	-	2
	10+ services	-	-	-

AGENCY	RELEVANT STATISTICS	NUMBER OF SERVICES		
		07/08	08/09	09/10
TAS POLICE	1 service only	-	-	-
	2 – 5 services	-	1	1
	6 – 10 services	-	-	-
	10+ services	-	-	-
VIC POLICE	1 service only	24	12	9
	2 – 5 services	60	46	67
	6 – 10 services	6	8	9
	10+ services	-	-	2
WA POLICE	1 service only	5	5	11
	2 – 5 services	17	19	34
	6 – 10 services	8	5	7
	10+ services	-	3	1
TOTAL [paragraph 100(2)(eb)]	**1 service only**	**117**	**79**	**95**
	2 – 5 services	**293**	**306**	**383**
	6 – 10 services	**52**	**44**	**55**
	10+ services	**10**	**5**	**5**

4.20 Paragraphs 100(1)(ec) and 100(2)(ec) of the TIA Act provide that the report must include, for each agency and in total, the total number of services intercepted under service based named person warrants and the number of devices intercepted under a device based named person warrant. This information is presented in Tables 11 and 12.

Table 11—Total number of services intercepted under *service* based named person warrants

AGENCY	TOTAL NUMBER OF SERVICES INTERCEPTED	
	08/09	09/10
ACC	285	311
AFP	416	459
CCC WA	8	6
CMC	-	22
ICAC	2	4
NSW CC	209	181
NSW POLICE	70	75
NT POLICE	25	28
OPI	37	2
PIC	22	6
QLD POLICE	-	68
SA POLICE	9	78
TAS POLICE	3	5
VIC POLICE	225	296
WA POLICE	150	175
TOTAL	**1,461**	**1,716**

Table 12—Total number of services and devices intercepted under *device* based named person warrants

AGENCY	SERVICES		DEVICES	
	08/09	09/10	08/09	09/10
AFP	-	-	16	12
NSW CC	-	1	-	5
NSW POLICE	-	2	1	7
QLD POLICE	-	-	-	2
VIC POLICE	-	-	1	-
TOTAL	**-**	**3**	**18**	**26**

B-Party warrants

4.21 Paragraphs 100(1)(ed) of the TIA Act provides that the report must include the same statistics outlined above in relation to warrants where subparagraph 46(1)(d)(ii) applied, being B-Party warrants. This means that the following statistics must be provided:

- the number of B-Party warrants applied for, refused and issued
- the number of telephone applications for B-Party warrants made, refused and issued
- the number of renewal applications for B-Party warrants made, refused and issued
- the number of B-Party warrants which authorise entry onto premises, and

- the number of B-Party warrants issued with conditions or restrictions attached.

4.22 Paragraph 100(2)(ed) of the TIA Act provides that the report must also include these statistics in total across all agencies. Tables 13 to 16 set out the information supplied by intercepting agencies regarding B-Party warrants. There has been a 64% increase of applications for B-Party warrants since the last reporting period. This increase can be attributed to the operational needs of agencies.

4.23 No B-Party warrants authorised entry onto premises during the reporting period.

Table 13—Applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		07/08	08/09	09/10
ACC	Made	2	1	-
	Refused/withdrawn	-	-	-
	Issued	2	1	-
AFP	Made	15	8	43
	Refused/withdrawn	-	-	-
	Issued	15	8	43
CCC WA	Made	3	-	1
	Refused/withdrawn	-	-	-
	Issued	3	-	1
ICAC	Made	3	1	-
	Refused/withdrawn	-	-	-
	Issued	3	1	-
NSW CC	Made	22	13	4
	Refused/withdrawn	-	-	-
	Issued	22	13	4
NSW POLICE	Made	26	40	38
	Refused/withdrawn	-	-	-
	Issued	26	40	38
OPI	Made	10	3	-
	Refused/withdrawn	-	-	-
	Issued	10	3	-
QLD POLICE	Made	-	-	1
	Refused/withdrawn	-	-	-
	Issued	-	-	1
SA POLICE	Made	-	2	-
	Refused/withdrawn	-	-	-
	Issued	-	2	-
VIC POLICE	Made	15	5	32
	Refused/withdrawn	-	-	-
	Issued	15	5	32
WA POLICE	Made	-	-	1
	Refused/withdrawn	-	-	-
	Issued	-	-	1
TOTAL [paragraph 100(2)(ed)]	**Made**	**96**	**73**	**120**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**96**	**73**	**120**

Table 14—Telephone applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		07/08	08/09	09/10
AFP	Made	-	-	3
	Refused/withdrawn	-	-	-
	Issued	-	-	3
NSW POLICE	Made	7	5	8
	Refused/withdrawn	-	-	-
	Issued	7	5	8
VIC POLICE	Made	2	-	-
	Refused/withdrawn	-	-	-
	Issued	2	-	-
TOTAL [paragraph 100(2)(ed)]	**Made**	**9**	**5**	**11**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**9**	**5**	**11**

Table 15—Renewal applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		07/08	08/09	09/10
AFP	Made	1	4	26
	Refused/withdrawn	-	-	-
	Issued	1	4	26
NSW CC	Made	2	-	-
	Refused/withdrawn	-	-	-
	Issued	2	-	-
NSW POLICE	Made	-	2	4
	Refused/withdrawn	-	-	-
	Issued	-	2	4
VIC POLICE	Made	8	-	15
	Refused/withdrawn	-	-	-
	Issued	8	-	15
TOTAL [paragraph 100(2)(ed)]	**Made**	**11**	**6**	**45**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**11**	**6**	**45**

Table 16— B-Party warrants issued with conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		07/08	08/09	09/10
ICAC	Issued	-	1	-
TOTAL [paragraph 100(2)(ed)]	**Issued**	**-**	**1**	**-**

Interpretative note relating to B-Party warrants

4.24 These statistics demonstrate that B-Party warrants are only used sparingly. Of the sixteen agencies that were issued telecommunications interception warrants during the reporting period, only eleven applied for and were issued B-Party warrants, with B-Party warrants representing approximately 3% of the total number of warrants issued.

4.25 It is important to note that only 45 of the 120 B-Party warrants were renewed, meaning that agencies recognise the primary purpose of B-Party warrants, which is a mechanism for identifying the telecommunications services, identity or location of the suspect.

Categories of serious offences specified in telecommunications interception warrants

4.26 Paragraph 100(1)(f) of the TIA Act provides that the report must set out the categories of serious offences specified in telecommunications interception warrants issued to each agency during the reporting period. Paragraph 100(1)(g) of the TIA Act provides that the report must set out the number of serious offences in each category that were so specified.

4.27 The information required by paragraphs 100(1)(f) and (g) is set out in Tables 17 to 32. As in previous years, agencies obtained the majority of warrants to assist with investigations into drug-related offences.

4.28 Care should be taken in interpreting the following table as warrants may have been issued in the investigation of more than one serious offence. The data for each serious offence includes figures for any related ancillary offences, such as assisting in the commission of, or conspiring to commit, a principal offence.

Table 17—Categories of serious offences specified in telecommunications interception warrants issued to the ACC

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
ACC special investigations	160	153	210
Serious drug offences	16	1	-
Serious fraud or loss of revenue	3	-	-

Table 18—Categories of serious offences specified in telecommunications interception warrants issued to ACLEI

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the *Criminal Code Act 1995*	-	-	1

Table 19—Categories of serious offences specified in telecommunications interception warrants issued to the AFP

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Bribery or corruption	-	1	1
Child pornography	-	-	3
Cybercrime	1	3	3
Kidnapping	4	4	-
Money laundering	106	104	136
Murder	2	21	16
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the *Criminal Code Act 1995*	3	-	2
Offences involving planning and organisation	16	26	13
People smuggling or sexual servitude	5	19	30
Serious damage to property	5	-	-
Serious drug offences	361	282	391
Serious fraud or loss of revenue	13	12	18
Serious personal injury or loss of life	14	27	73
Terrorism	10	91	141
Telecommunications offences	3	11	17

Table 20—Categories of serious offences specified in telecommunications interception warrants issued to the CCC WA

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Bribery or corruption	102	19	39
Child pornography	-	10	-
Cybercrime	3	27	4
Serious drug offences	-	11	-

Table 21—Categories of serious offences specified in telecommunications interception warrants issued to the CMC

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Bribery or corruption	-	-	7
Serious drug offences	-	-	11

Table 22—Categories of serious offences specified in telecommunications interception warrants issued to the ICAC

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Bribery or corruption	30	32	14
Serious fraud or loss of revenue	3	-	-

Table 23—Categories of serious offences specified in telecommunications interception warrants issued to the NSW CC

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Cybercrime	-	6	-
Kidnapping	-	9	-
Money laundering	142	26	61
Murder	64	47	61
Offences involving planning and organisation	40	33	24
Serious damage to property	13	-	-
Serious drug offences	474	478	228
Serious fraud or loss of revenue	27	24	10
Serious personal injury or loss of life	16	16	20

Table 24—Categories of serious offences specified in telecommunications interception warrants issued to the NSW Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Bribery or corruption	33	10	15
Child pornography	5	-	-
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	2
Kidnapping	27	14	22
Murder	231	237	293
Offences involving planning and organisation	120	165	152
Serious arson	-	-	9
Serious damage to property	57	30	20
Serious drug offences	145	147	389
Serious fraud or loss of revenue	7	19	46
Serious personal injury or loss of life	208	194	164
Terrorism	19	10	29

Table 25—Categories of serious offences specified in telecommunications interception warrants issued to NT Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Murder	4	3	7
Offences involving planning and organisation	1	-	-
Serious drug offences	32	42	43
Serious personal injury or loss of life	2	-	-

Table 26—Categories of serious offences specified in telecommunications interception warrants issued to the OPI

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Bribery or corruption	68	58	36
Murder	11	-	-
Serious drug offences	1	-	-
Serious personal injury or loss of life	-	7	-

Table 27—Categories of serious offences specified in telecommunications interception warrants issued to the PIC

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Bribery or corruption	65	98	41
Money laundering	11	7	-
Offences involving planning and organisation	3	-	-
Serious drug offences	1	10	3
Serious personal injury or loss of life	12	-	4

Table 28—Categories of serious offences specified in telecommunications interception warrants issued to the QLD Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	-	11
Murder	-	-	26
Offences involving planning and organisation	-	-	7
Serious arson	-	-	1
Serious drug offences	-	-	115
Serious fraud or loss of revenue	-	-	7
Serious personal injury or loss of life	-	-	9

Table 29—Categories of serious offences specified in telecommunications interception warrants issued to the SA Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Administration of justice[3]	-	4	-
Bribery or corruption	4	-	5
Child pornography	-	-	6
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	16
Cybercrime	-	3	-
Kidnapping	1	-	-
Money Laundering	-	-	4
Murder	37	23	17
Serious arson	-	1	-
Serious damage to property	3	-	-
Serious drug offences	71	65	90
Serious fraud or loss of revenue	-	6	1
Serious personal injury or loss of life	8	3	14

Table 30—Categories of serious offences specified in telecommunications interception warrants issued to Tas Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Bribery or corruption	3	-	-
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	1
Murder	3	2	17
Serious drug offences	5	8	8
Serious fraud or loss of revenue	3	-	-
Serious personal injury of loss of life	3	5	-

[3] This refers to offences against sections 35, 36, 36A, 37, 39, 41, 42, 43, 46 or 47 of the *Crimes Act 1914*.

Table 31—Categories of serious offences specified in telecommunications interception warrants issued to the Vic Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Bribery or corruption	-	28	4
Kidnapping	1	3	11
Money Laundering	-	-	1
Murder	118	63	113
Offences involving planning and organisation	4	-	-
Serious arson	-	2	3
Serious damage to property	6	-	-
Serious drug offences	180	170	191
Serious fraud or loss of revenue	3	-	-
Serious personal injury or loss of life	61	65	65

Table 32—Categories of serious offences specified in telecommunications interception warrants issued to the WA Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
Bribery or corruption	5	9	-
Child pornography	-	9	-
Kidnapping	-	8	8
Money laundering	5	1	3
Murder	29	38	34
Offences involving planning and organisation	2	2	14
Serious arson	-	-	10
Serious damage to property	2	-	1
Serious drug offences	134	177	209
Serious fraud or loss of revenue	7	11	-
Serious personal injury or loss of life	15	32	46

Interpretative note relating to categories of serious offences specified in telecommunications interception warrants

4.29 Offence involving planning and organisation (subsection 5D(3) of the TIA Act) were previously categorised as organised crime. With the introduction of offences relating to criminal organisations and associations in the SOC2 Act, the categories have been updated. These SOC2 Act offences are now categorised as organised crime.

Categories of serious offences specified in telecommunications interception warrants – all agencies

4.30 Paragraphs 100(2)(f) and (g) of the TIA Act provide that the categories of serious offences specified in telecommunications interception warrants for all agencies must be set out in combined form. This information is set out in Table 33.

Table 33—Categories of serious offences specified in telecommunications interception warrants in relation to all agencies

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	07/08	08/09	09/10
ACC special investigations[4]	160	153	210
Administration of justice[5]	-	4	-
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	-	11
Bribery or corruption	310	255	162
Child pornography	5	19	9
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	19
Cybercrime	4	39	7
Kidnapping	33	38	41
Money laundering	264	138	205
Murder	499	434	584
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the *Criminal Code Act 1995*	3	-	3
Offences involving planning and organisation	186	226	210
People smuggling or sexual servitude	5	19	30
Serious arson	-	3	13
Serious damage to property	86	30	21
Serious drug offences	1420	1391	1678
Serious fraud or loss of revenue	66	72	82
Serious personal injury or loss of life	339	349	395
Telecommunications offences	3	11	17
Terrorism	29	101	170

[4] Applies only to the ACC.

[5] This refers to offences against sections 35, 36, 36A, 37, 39, 41, 42, 43, 46 or 47 of the *Crimes Act 1914*

Duration of telecommunications interception warrants

4.31 Section 49 of the TIA Act provides that a telecommunications interception warrant must specify the period for which it is to be in force. Warrants may be revoked before the specified period lapses. Section 57 of the TIA Act provides that the chief officer of an agency must revoke a warrant where he or she is satisfied that the grounds on which the warrant was issued have ceased to exist.

Duration of original telecommunications interception warrants

4.32 Paragraph 101(1)(a) of the TIA Act provides that the report must set out the average period specified in original telecommunications interception warrants in relation to each agency. Paragraph 101(1)(b) provides that the report must set out the average of the periods for which those warrants were actually in force. Paragraphs 101(2)(a) and (b) provide that the same information must be averaged across all agencies. This information is set out in Table 34.

4.33 The average duration specified in warrants, has increased, however the actual duration of warrants has reduced. The average duration has increased for some agencies while it has decreased for others, meaning that there is no general trend relating to the duration of warrants.

4.34 As in previous reporting periods, the average actual duration of warrants is again significantly less than the average specified duration of warrants, meaning that agencies continue to regularly review warrants and revoke those that are no longer required prior to their expiration. This demonstrates that agencies do not intercept telecommunications services longer than they need to for their investigations.

Table 34—Duration of original telecommunications interception warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	07/08	08/09	09/10	07/08	08/09	09/10
ACC	87	89	86	57	62	45
ACLEI	-	-	25	-	-	25
AFP	77	73	80	41	49	54
CCC WA	77	90	73	49	80	64
CMC	-	-	53	-	-	48
ICAC	79	83	90	61	55	84
NSW CC	82	85	84	53	52	71
NSW POLICE	46	49	61	37	46	52
NT POLICE	83	86	86	69	66	61
OPI	76	70	55	67	44	47
PIC	88	89	90	77	76	69
QLD POLICE	-	-	40	-	-	31
SA POLICE	82	74	83	55	61	64
TAS POLICE	54	74	84	18	46	68
VIC POLICE	52	52	55	37	43	41
WA POLICE	64	62	86	41	39	48
AVERAGE [paragraphs 101(2)(a)-(b)]	**68**	**69**	**71**	**46**	**55**	**52**

Duration of renewal telecommunications interception warrants

4.35 Paragraphs 101(1)(c), (1)(d), (2)(c) and (2)(d) of the TIA Act provide that the report set out corresponding information in relation to telecommunications interception warrants that have been renewed. This information is set out in Table 35. There is no substantial variation in the average specified or actual durations of renewal warrants from previous reporting periods.

Table 35—Duration of renewal of telecommunications interception warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	07/08	08/09	09/10	07/08	08/09	09/10
ACC	90	83	76	71	68	79
AFP	89	87	83	73	73	66
CCC WA	90	83	73	71	85	153
CMC	-	-	65	-	-	61
ICAC	74	90	90	51	22	17
NSW CC	76	86	102	54	60	68
NSW POLICE	52	55	66	59	47	64
NT POLICE	-	90	81	-	90	45
OPI	85	45	-	84	41	-
PIC	90	90	90	83	71	88
QLD POLICE	-	-	42	-	-	32
SA POLICE	90	60	90	42	60	-
TAS POLICE	-	-	90	-	-	90
VIC POLICE	55	59	59	48	52	40
WA POLICE	68	64	74	61	49	53
AVERAGE [paragraphs 101(2)(a)-(b)]	**74**	**74**	**75**	**62**	**56**	**63**

Interpretative note relating to average duration of warrants across all agencies

4.36 The figures in Tables 34 and 35 reflect the average durations, both specified and actual, for all original and renewal warrants issued to all agencies.

4.37 These figures illustrate that the duration of warrants is generally consistent from year to year, and that the actual duration of warrants is typically shorter than the specified duration.

Duration of original B-Party warrants

4.38 As with all telecommunications interception warrants, a B-Party warrant must specify the period for which it is to be in force and may be revoked before the specified period lapses. The obligation on the chief officer of an agency to revoke a B-Party warrant where he or she is satisfied that the grounds on which the warrant was issued have ceased to exist is particularly important in the case of B-Party warrants.
For example, if a B-Party warrant was issued because the telecommunications service of the target was not able to be identified, once the service is identified, the warrant must be revoked.

4.39 Paragraph 101(1)(da) of the TIA Act provides that the report must set out the average period specified in original B-Party warrants in relation to each agency and the average of the periods for which those warrants were actually in force.
Paragraph 101(2)(da) provides that the same information must be averaged across all agencies. This information is set out in Table 36.

Table 36—Duration of original B-Party warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	07/08	08/09	09/10	07/08	08/09	09/10
ACC	26	45	-	4	13	-
AFP	36	45	45	19	44	33
CCC WA	45	-	45	15	-	38
ICAC	15	45	-	15	45	-
NSW CC	42	42	45	28	15	32
NSW POLICE	22	27	34	18	18	25
OPI	45	34	-	16	21	-
QLD POLICE	-	-	8	-	-	8
SA POLICE	-	30	-	-	30	-
VIC POLICE	34	45	45	25	16	45
WA POLICE	-	-	14	-	-	14
AVERAGE [paragraph 101(2)(da)]	**33**	**34**	**34**	**23**	**21**	**28**

Duration of renewal B-Party warrants

4.40 Paragraphs 101(1)(da) and (2)(da) of the TIA Act also provide that the report must set out corresponding information in relation to B-Party warrants that have been renewed. This information is set out in Table 37.

Table 37—Duration of renewal of B-Party warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	07/08	08/09	09/10	07/08	08/09	09/10
AFP	45	45	46	40	42	47
NSW CC	44	-	-	32	-	-
NSW POLICE	-	30	29	-	29	29
VIC POLICE	45	-	45	45	-	29
AVERAGE [paragraphs 101(2)(da)]	**45**	**40**	**40**	**42**	**38**	**35**

Number of final renewals of telecommunications interception warrants

4.41 Paragraph 101(1)(e) of the TIA Act provides that the report must record the number of final renewals that ceased to be in force during the reporting period. A final renewal refers to a telecommunications interception warrant that is the last renewal of an original warrant, and is recorded in terms of the number of days after the date of issue of the original warrant that the final renewal ceases to be in force. The categories of final renewals are as follows:

- 90 day final renewal—a last renewal that ceases to be in force more than 90 days but not more than 150 days after the date of issue of the original warrant
- 150 day final renewal—a last renewal that ceases to be in force more than 150 days but not more than 180 days after the date of issue of the original warrant, and
- 180 day final renewal—a last renewal that ceases to be in force more than 180 days after the date of issue of the original warrant.

4.42 This information gives some indication of the overall duration of warrants that have been renewed. Paragraph 101(2)(e) of the Act provides that the same information must be set out in total across all agencies. This information is set out in Table 38.

4.43 The figures in Table 38 show an increase in 90 day renewals, and a decrease in 150 day and 180 day renewals. This is consistent with operational activities.

Table 38—Number of 'final renewals'

AGENCY	90 DAYS			150 DAYS			180 DAYS		
	07/08	08/09	09/10	07/08	08/09	09/10	07/08	08/09	09/10
ACC	7	7	6	14	7	4	10	7	6
AFP	10	18	4	30	24	21	31	37	24
CCC WA	5	-	3	1	-	-	10	-	-
ICAC	4	2	3	2	-	-	-	-	-
NSW CC	4	6	7	3	7	4	3	2	5
NSW POLICE	41	50	74	7	6	4	2	11	5
NT POLICE	-	-	3	-	-	-	-	1	1
OPI	3	1	8	3	-	-	7	-	9
PIC	2	8	-	-	8	-	1	5	-
QLD POLICE	-	-	4	-	-	-	-	-	-
SA POLICE	3	2	-	-	1	-	-	-	-
TAS POLICE	-	-	-	-	-	-	-	-	-
VIC POLICE	18	17	24	9	2	5	1	2	2
WA POLICE	7	13	19	1	28	12	10	1	3
TOTAL [paragraph 101(2)(e)]	**104**	**124**	**155**	**70**	**83**	**50**	**75**	**66**	**55**

Effectiveness of telecommunications interception warrants

4.44 Section 102 of the TIA Act provides that the report must include information about the effectiveness of telecommunications interception warrants. Specifically, the report must state how many arrests were made on the basis of information obtained by intercepting a communication under a telecommunications interception warrant.

4.45 The report must also include information about prosecutions for 'prescribed offences' in which lawfully intercepted information was given in evidence and the number of those in respect of which convictions were recorded. The term 'prescribed offence' is defined in subsection 5(1) of the TIA Act to mean:

- a serious offence
- an offence against subsection 7(1) of the TIA Act, which prohibits the interception of telecommunications
- an offence against section 63 of the TIA Act, which prohibits the communication, recording or use of intercepted information
- an offence against subsection 108(1) of the TIA Act, which prohibits the accessing of stored communications
- an offence against section 133 of the TIA Act, which prohibits the communication, recording or use of lawfully accessed information
- an offence against a provision of Part 10.6 of the Criminal Code, which deals with the protection of telecommunications networks and installations
- any other offence punishable by imprisonment for life or for a period, or maximum period, of at least 3 years, or
- an ancillary offence relating to an offence of a kind referred to above.

4.46 Figures for the number of arrests for prescribed offences in which lawfully intercepted information was given in evidence are provided in respect of all eligible authorities and eligible Commonwealth authorities. While only eligible authorities that are interception agencies for the purposes of the TIA Act may obtain warrants, information obtained under such warrants may in some circumstances be communicated to another eligible authority that is not an interception agency.

4.47 The communication of that information may result in further investigation and possibly arrests and prosecution by an eligible authority on the basis of lawfully intercepted information. That is notwithstanding that the authority is itself unable to obtain a warrant. An example of such a situation might be the interception under warrant by a Commonwealth agency of information pointing to the commission of a State offence where the police force of that State has not been declared to be an interception agency for the purposes of the TIA Act but is an eligible authority. In these circumstances, it may be possible for the Commonwealth agency to communicate the information to the State police service in accordance with Part 2-6 of the TIA Act.

4.48 Eligible authorities that were not interception agencies for the purposes of the TIA Act during the reporting period are:

- the Inspector of the Police Integrity Commission
- the Inspector of the Independent Commission against Corruption, and
- the Parliamentary Inspector of the Corruption and Crime Commission of Western Australia.

Arrests on the basis of lawfully intercepted information

4.49 Paragraph 102(1)(a) of the TIA Act provides that the report must set out, for each agency and eligible authority, how many arrests were made in connection with the performance by the agency or authority of its functions and on the basis of information that was or included lawfully intercepted information during the reporting period.

4.50 Paragraph 102(2)(a) provides that the total number of arrests across agencies and eligible authorities must be reported. This information is set out in Table 39. The number of arrests made during the reporting period represents a 12% increase on the figures reported during 2008-09.

Table 39—Arrests on the basis of lawfully intercepted information

AGENCY	NUMBER OF ARRESTS		
	07/08	08/09	09/10
ACC	166	133	72
AFP	165	133	116
CCC WA	3	1	1
CMC	231	-	52
ICAC	-	-	2
NSW CC	306	175	135
NSW POLICE	321	402	429
NT POLICE	27	31	48
OPI	-	1	-
PIC	85	139	189
QLD POLICE	18	48	268
SA POLICE	67	89	176
TAS POLICE	7	9	54
VIC POLICE	493	420	371
WA POLICE	167	134	-
TOTAL [paragraph 102(2)(a)]	**2,056**	**1,715**	**1,913**

Prosecutions in which lawfully intercepted information was given in evidence

4.51 Paragraphs 102(1)(b) and (c) of the TIA Act provide that the report must set out, for each agency and each eligible authority, the categories of prescribed offences prosecuted, and the number of offences in each category, in which lawfully intercepted information was given in evidence, and the number of offences in each category in respect of which convictions were recorded. Paragraphs 102(2)(b) and (c) provide that this information must be set out in total across all agencies and eligible authorities. The information required is set out in Tables 40 to 42.

4.52 During the reporting period, there was a 9% decrease in the number of prosecutions commenced, but a 4% increase in the number of convictions obtained on the basis of lawfully intercepted information.

4.53 It should be noted that the statistics do not necessarily relate to lawfully intercepted information obtained under telecommunications interception warrants issued in the current reporting period as information obtained may be used in later reporting periods.

4.54 In these tables, the category 'other offences' refers to any other offence punishable by imprisonment for life or for a period of at least three years, or to any related ancillary offences.

Table 40—Prosecutions in which lawfully intercepted information used in evidence

CATEGORIES OF OFFENCES	ACC	AFP	CCC WA	ICAC	NSW CC	NSW POL	NT POL	OPI	PIC	QLD POL	SA POL	VIC POL	WA POL	TOTAL
Administration of Justice									4					**4**
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence					1							17		**18**
Bribery or corruption			65	3		2		2	1		3	6		**82**
Child pornography		2				3						2	1	**8**
Conspiring to commit or aiding or abetting the commission of a serious offence		2			1	2			2				4	**11**
Cybercrime			58											**58**
Kidnapping					1	9						6	2	**18**
Money laundering	2	7			22						1	2		**34**
Murder		1			2	44	6					13	2	**68**
Offences involving planning and organisation					107	163						41	87	**398**
Serious arson						3							4	**7**
Serious damage to property					2	6							9	**17**
Serious drug offences	5	79			191	574	15			18		252	434	**1568**
Serious fraud or loss of revenue	5	2			16	102					39		1	**165**
Serious personal injury/ loss of life					33	241					1	64	1	**340**
Special Investigation of the ACC	64													**64**
Terrorism		3			9									**12**
Other offences		1				46			15	1	4	90	50	**207**
TOTAL	**76**	**97**	**123**	**3**	**385**	**1195**	**21**	**2**	**22**	**19**	**48**	**493**	**595**	**3079**

Table 41—Convictions in which lawfully intercepted information given in evidence

CATEGORIES OF OFFENCES	ACC	AFP	CCC WA	NSW CC	NSW POL	NT POL	OPI	PIC	QLD POL	SA POL	TAS POL	VIC POL	WA POL	TOTAL
Administration of Justice								3						**3**
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence				1								17		**18**
Bribery or corruption			60		2		1	1				6		**70**
Child pornography		1			3							2	1	**7**
Conspiring to commit or aiding or abetting the commission of a serious offence		1		1	2			1						**5**
Cybercrime			58											**58**
Kidnapping				1	6							6		**13**
Money laundering				19						1		2		**22**
Murder					29	5						12	2	**48**
Offences involving planning and organisation				36	113							41	29	**219**
Serious arson												21		**21**
Serious damage to property				2	6								4	**12**
Serious drug offences	5	20		183	507	12			6	35	18	250	83	**1119**
Serious fraud or loss of revenue	2			16	112									**130**
Serious personal injury/ loss of life				18	190							61	1	**270**
Special Investigation of the ACC	10													**10**
Terrorism		9		9										**18**
Other offences	1				35			7	1	4		87	20	**155**
TOTAL	**18**	**31**	**118**	**286**	**1005**	**17**	**1**	**12**	**7**	**40**	**18**	**505**	**140**	**2198**

Table 42—Prosecutions and convictions in which lawfully intercepted information given in evidence

AGENCY	CATEGORIES OF OFFENCES PROSECUTED	NUMBER OF OFFENCES PROSECUTED FOR EACH CATEGORY			NUMBER OF CONVICTIONS RECORDED FOR EACH CATEGORY		
		07/08	08/09	09/10	07/08	08/09	09/10
ACC	Serious Offence	55	30	76	52	23	17
	Other[6]	5	32	-	5	6	1
	Agency Total	60	62	76	57	29	18
AFP	Serious Offence	136	168	96	14	23	31
	Other	6	11	1	-	-	-
	Agency Total	142	179	97	14	23	31
CCC WA	Serious Offence	3	21	123	3	8	118
	Other	2	-	-	2	-	-
	Agency Total	5	21	123	5	8	118
CMC	Serious Offence	231	-	-	49	-	-
	Other	26	-	-	12	-	-
	Agency Total	257	-	-	61	-	-
ICAC	Serious Offence	-	-	3	-	-	-
	Other	-	28	-	-	8	-
	Agency Total	-	28	3	-	8	-
NSW CC	Serious Offence	736	342	385	734	246	286
	Other	-	-	-	-	-	-
	Agency Total	736	342	385	734	246	286
NSW POLICE	Serious Offence	1,428	1,234	1,149	629	774	970
	Other	-	76	46	-	59	35
	Agency Total	1,428	1,310	1,195	629	833	1,005
NT POLICE	Serious Offence	21	11	21	9	9	17
	Other	-	-	-	-	-	-
	Agency Total	21	11	21	9	9	17
OPI	Serious Offence	-	8	2	-	5	1
	Other	-	-	-	-	-	-
	Agency Total	-	8	2	-	5	1
PIC	Serious Offence	20	13	7	20	12	5
	Other	8	20	15	8	14	7
	Agency Total	28	33	22	28	26	12
QLD POLICE	Serious Offence	20	11	18	2	-	6
	Other	-	4	1	-	-	1
	Agency Total	20	15	19	2	-	7
SA POLICE	Serious Offence	60	138	44	45	46	36
	Other	8	2	4	8	7	4
	Agency Total	68	140	48	53	53	40
TAS POLICE	Serious Offence	4	9	-	-	-	18
	Other	-	-	-	-	-	-
	Agency Total	4	9	-	-	-	18
VIC POLICE	Serious Offence	295	348	403	280	342	418
	Other	167	77	90	162	76	87
	Agency Total	462	425	493	442	418	505
WA POLICE	Serious Offence	666	755	545	503	415	120
	Other	19	82	50	5	36	20
	Agency Total	685	837	595	508	451	140
TOTAL	**Serious Offence**	**3,675**	**3,088**	**2,872**	**2,340**	**1,903**	**2,043**
	Other	**241**	**332**	**207**	**202**	**206**	**155**
	Grand Total	**3,916**	**3,420**	**3,079**	**2,255**	**2,109**	**2,198**

[6] The 'Other' offences here refer to those offences that are not 'serious offences' (i.e. offences for which a telecommunications interception warrant can be obtained) but whose investigation is able to be furthered through the use of lawfully intercepted information. It also includes offences of dishonesty such as theft and offences against the administration of justice.

Interpretative note relating to prosecutions and convictions statistics

4.55 The statistics presented in Tables 40 to 42 should be interpreted with some caution, particularly in presuming a relationship between the number of arrests, prosecutions (which include committal proceedings) and convictions in a reporting period. An arrest recorded in one reporting period may not result in a prosecution/committal (if at all) until a later reporting period and any resulting conviction may be recorded in that or an even later reporting period. Additionally, the number of arrests may not equate to the number of charges laid as an arrested person may be prosecuted and convicted for a number of offences, some or all of which may be prosecuted at a later time.

4.56 Further, the tables may understate the effectiveness of interception in so far as, in some cases, prosecutions may be initiated, and convictions recorded, without the need to give intercepted information in evidence. In particular, agencies report that telecommunications interception effectively enables investigators to identify persons involved in, and the infrastructure of, organised criminal activities, particularly drug trafficking syndicates. In many cases, the weight of evidence obtained through telecommunications interception results in defendants entering guilty pleas, thereby obviating the need for the information to be introduced into evidence.

Percentage of 'eligible warrants'

4.57 Subsections 102(3) and (4) of the TIA Act provide that the report must include information that provides a general indication of the proportion of telecommunications interception warrants that provide information which is used in the prosecution of an offence.

4.58 Subsection 102(3) of the TIA Act provides that the report must set out the number of eligible warrants issued to each agency during the reporting period and the percentage of warrants issued to that agency that were eligible warrants. An 'eligible warrant' is defined in subsection 102(3) as a warrant that was in force during the reporting period (not necessarily a warrant that was issued during the reporting period) where a prosecution was instituted or was likely to be instituted on the basis of information obtained by interceptions under the warrant.[7]

4.59 Subsection 102(4) of the TIA Act provides that the report must set out the percentage of each agency's total warrants in force during the reporting period, that were eligible warrants. These figures are set out in Table 43, and indicate a 1% decrease in the proportion of eligible warrants when compared to the previous reporting period.

[7] If the warrant was a renewal, this includes information obtained under the original or any renewal of the original warrant; if the warrant was an original warrant, this includes information obtained under any renewal of that original warrant.

Table 43—Percentage of 'eligible warrants'

AGENCY	NUMBER OF ELIGIBLE WARRANTS		TOTAL NUMBER OF WARRANTS		%	
	08/09	09/10	08/09	09/10	08/09	09/10
ACC	167	193	176	222	95	87
AFP	415	542	814	754	51	72
CCC WA	39	29	52	50	75	58
CMC	-	15	-	15	-	100
ICAC	22	7	32	7	69	100
NSW CC	589	392	724	438	81	90
NSW POLICE	741	869	927	1233	80	70
NT POLICE	44	44	52	51	85	86
OPI	32	1	64	36	50	3
PIC	46	16	139	63	33	25
QLD POLICE	-	159	-	172	-	92
SA POLICE	83	110	105	116	79	95
TAS POLICE	5	6	12	15	42	40
VIC POLICE	287	291	375	420	77	69
WA POLICE	265	105	312	307	85	34
TOTAL [subsection 102(4)]	**2,735**	**2,779**	**3,784**	**3,899**	**72**	**71**

Emergency interception

4.60 Section 102A of the TIA Act provides that the report must set out the number of occasions on which an officer or staff member of the agency intercepted a communication in reliance on subsection 7(4) or (5) of the TIA Act. These provisions permit the AFP or a police force of a State or the Northern Territory to intercept calls in emergencies such as sieges and, with appropriate consent, in kidnapping and extortion cases.

4.61 An interception in reliance on subsection 7(4) of the TIA Act may be carried out by an officer of one of the above agencies where the officer is a party to the communication, and because of the urgency of the need for the act to be done, it is not reasonably practicable for an application for a telecommunications interception warrant to be made. There also must be reasonable grounds for suspecting that the other party to the communication has:

- done an act that has resulted or may result in loss of life or the infliction of serious personal injury
- threatened to kill or seriously injure another person or to cause serious damage to property, or
- threatened to take his or her own life or to do an act that would or may endanger his or her own life or create a serious threat to his or her health or safety.

4.62 In the reporting period no interceptions were carried out in reliance on subsection 7(4).

4.63 Interception of communications carried out pursuant to subsection 7(5) of the TIA Act must have the consent of the person to whom the communication is directed, and must satisfy the same conditions specified for subsection 7(4).

4.64 In the reporting period two interceptions were carried out in reliance on subsection 7(5). The information required by section 102A is set out in Table 44.

Table 44—Interceptions made in reliance on subsection 7(5) of the TIA Act

SUSPICION OF	AFP			NSW POLICE		
	07/08	08/09	09/10	07/08	08/09	09/10
An act that may result in loss of life or serious injury	-	-	-	2	-	2
Threat to kill or seriously injure	2	-	-	-	-	-
TOTAL	**2**	**-**	**-**	**2**	**-**	**2**

Other information

Total expenditure incurred by agencies

4.65 Paragraph 103(a) of the TIA Act provides that the report include details of the total expenditure (including expenditure of a capital nature) incurred by agencies in connection with the execution of telecommunications interception warrants for law enforcement purposes. The information required by this subsection is set out in Table 45.

4.66 Total expenditure incurred by agencies in connection with telecommunications interception increased by approximately 10% from the previous reporting period. This includes the start up costs of the Crime and Misconduct Commission and Queensland Police.

Table 45—Total expenditure incurred by each agency in connection with the execution of telecommunications interception warrants

AGENCY	TOTAL EXPENDITURE ($)		
	07/08	08/09	09/10
ACC	5,078,973	5,767,648	5,437,135
ACLEI	-	-	7,460
AFP	8,256,034	8,221,162	9,586,423
CCC WA	1,638,018	1,817,120	1,520,265
CMC	-	-	1,254,984[8]
ICAC	236,021	214,446	153,907
NSW CC	4,274,442	4,473,035	4,063,904
NSW POLICE	4,268,907	8,019,292	5,296,367
NT POLICE	886,000	693,458	701,485
OPI	1,914,644	1,671,170	2,034,841
PIC	1,189,530	1,351,587	1,141,823
QLD POLICE	-	-	3,321,572[9]
SA POLICE	2,492,495	2,656,404	2,717,562
TAS POLICE	548,000	3,258	416,000
VIC POLICE	4,145,055	4,483,582	5,531,058
WA POLICE	1,810,687	2,816,442	3,116,737
TOTAL	**36,738,806**	**42,188,604**	**46,301,523**

[8] This figure includes first year costs for the CMC

[9] This figure includes first year costs for the Qld Police

Average expenditure per telecommunications interception warrant

4.67 Paragraph 103(aa) of the TIA Act provides that the report must set out for each agency the average amount spent on each telecommunications interception warrant worked out using the formula:

$$\frac{\text{Total warrant expenditure}}{\text{Number of warrants}}$$

where:

'Total warrant expenditure' is the total expenditure incurred by the agency in connection with the execution of warrants during the period to which the report relates; and

'Number of warrants' means the number of warrants to which the total warrant expenditure relates.

4.68 The average expenditure incurred by agencies per warrant over the reporting period is presented in Table 46.

Table 46—Average expenditure per telecommunications interception warrant

AGENCY	AVERAGE EXPENDITURE ($)		
	07/08	08/09	09/10
ACC	28,374	37,452	25,891
ACLEI	-	-	7,460
AFP	15,577	14,373	14,924
CCC WA	16,059	37,084	38,007
CMC	-	-	73,823
ICAC	7,152	6,701	10,993
NSW CC	6,361	7,226	11,073
NSW POLICE	5,264	9,650	4,642
NT POLICE	23,946	15,410	14,030
OPI	24,547	25,710	56,523
PIC	13,072	11,753	23,788
QLD POLICE	-	-	19,311
SA POLICE	20,101	25,299	24,049
TAS POLICE	32,235	217	20,800
VIC POLICE	11,113	13,546	14,225
WA POLICE	9,099	9,813	9,590

Availability of eligible judges and nominated AAT members

4.69 Paragraph 103(ab) of the TIA Act provides that the report must set out information about the availability of Judges to issue telecommunications interception warrants and the extent to which nominated AAT members have been used for that purpose. This information is set out in Tables 47 and 48.

Table 47—Availability of Federal Court Judges, Family Court Judges, Federal Magistrates and nominated AAT Members to issue telecommunications interception warrants[10]

ISSUING AUTHORITY	NUMBER ELIGIBLE
FEDERAL COURT JUDGES	11
FAMILY COURT JUDGES	12
FEDERAL MAGISTRATES	35
NOMINATED AAT MEMBERS	43

4.70 During the reporting period, approximately 77% of telecommunications interception warrants were issued by AAT members, 12% by Federal Magistrates, 9% by Family Court Judges and 1% by Federal Court Judges. The number of warrants issued by authorities is influenced by an agency's operational needs and the availability of an issuing authority at the time of application.

[10] The number eligible may be higher than the number eligible at any given time as the figure includes issuing authorities who may have retired and their replacements.

Table 48—Number of telecommunications interception warrants issued by Federal Court Judges, Family Court Judges, Federal Magistrates and nominated AAT members

AGENCY	ISSUING AUTHORITY			
	FEDERAL COURT JUDGES	FAMILY COURT JUDGES	FEDERAL MAGISTRATES	NOMINATED AAT MEMBERS
ACC	23	-	-	187
ACLEI	-	-	-	1
AFP	1	3	80	557
CCC WA	-	-	-	40
CMC	-	-	2	15
ICAC	-	-	-	14
NSW CC	-	-	32	336
NSW POLICE	-	11	110	1020
NT POLICE	-	-	23	27
OPI	-	-	-	36
PIC	-	-	9	39
QLD POLICE	-	-	163	9
SA POLICE	-	-	-	113
TAS POLICE	-	-	-	20
VIC POLICE	-	-	-	388
WA POLICE	-	305	-	20
TOTAL	**24**	**319**	**419**	**3,584**

Interceptions on behalf of other agencies

4.71 Paragraph 103(ac) of the TIA Act provides that the report must set out the number (if any) of interceptions carried out by each agency on behalf of other agencies. Table 49 sets out the number of interceptions executed by agencies on behalf of other agencies during the reporting period.

4.72 The main circumstances in which this type of interception occurs is where a larger agency assists a smaller agency to intercept to reduce the costs of the smaller agency, or where, due to a higher than usual number of warrants or a system failure, an agency is required to utilise another agency's facilities.

Table 49—Number of interceptions carried out on behalf of other agencies

INTERCEPTION CARRIED OUT BY	INTERCEPTION CARRIED OUT ON BEHALF OF	
VIC POLICE	**TASMANIA POLICE**	21
ACC	**QUEENSLAND POLICE**	215
ACC	**CMC**	33
AFP	**ACLEI**	1
TOTAL		**270**

Resources devoted to telecommunications interception

4.73 In addition to the total expenditure figures provided in Table 45, the figures in Table 50 below were supplied by each agency and provide a breakdown of the total recurrent costs of interception over the reporting period. However, as agencies do not necessarily treat particular items of expenditure in the same way, caution should be exercised in comparing costs incurred by individual agencies.

Table 50—Recurrent costs of interceptions per agency

AGENCY	SALARIES	ADMINISTRATIVE SUPPORT	CAPITAL EXPENDITURE	INTERCEPTION COSTS	TOTAL ($)
ACC	4,426,881	421,649	99,879	488,726	**5,437,135**
ACLEI	7,460	-	-	-	**7,460**
AFP	6,285,684	572,585	1,297,032	1,411,122	**9,566,423**
CCC WA	1,351,286	-	-	168,979	**1,520,265**
CMC	921,223	33,897	264,479	35,385	**1,254,984**
ICAC	38,856	-	64,247	50,804	**153,907**
NSW CC	2,059,614	88,877	684,801	1,230,612	**4,063,904**
NSW POLICE	3,467,740	480,027	772,996	575,604	**5,296,367**
NT POLICE	543,813	9,754	-	147,918	**701,485**
OPI	1,144,280	155,722	459,148	275,691	**2,034,841**
PIC	1,095,428[11]	-	-	46,395	**1,141,823**
QLD POLICE	1,530,481	61,774	115,384	1,613,933	**3,321,572**
SA POLICE	2,194,291	239,271	188,010	95,990	**2,717,562**
TAS POLICE	285,000	-	44,000	87,000	**416,000**
VIC POLICE	4,183,146	465,814	389,933	492,165	**5,531,058**
WA POLICE	2,775,363	212,301	-	129,073	**3,116,737**

[11] Administrative support is included in the salary figure for the PIC.

Emergency services facility declarations

4.74 Paragraph 103(ad) of the TIA Act provides that the report must include the number and type of premises for each State and Territory that have been declared by the Attorney-General to be emergency services facilities pursuant to subsection 6(2A) of the TIA Act during the reporting period. The declarations enable such facilities to record incoming and outgoing calls without a telecommunications interception warrant. Table 51 provides the required information.

Table 51—Emergency service facility declarations

STATE/TERRITORY	POLICE	FIRE BRIGADE	AMBULANCE	DESPATCHING
AUSTRALIAN CAPITAL TERRITORY	4	0	0	1
NEW SOUTH WALES	8	4	6	1
VICTORIA	6	1	10	4
SOUTH AUSTRALIA	1	2	1	0
WESTERN AUSTRALIA	1	2	1	0
TASMANIA	1	2	1	0
QUEENSLAND	21	12	9	0
NORTHERN TERRITORY	3	1	2	1
TOTAL	**45**	**24**	**30**	**7**

Reports by Commonwealth Ombudsman

4.75 The Commonwealth Ombudsman has the function of inspecting the records of Commonwealth interception agencies and reporting to the Attorney-General regarding the outcome of those inspections. Paragraph 103(ae) of the TIA Act provides that a summary of the information included in the Ombudsman's report must be included in this report, including:

- a summary of the inspections conducted during the financial year under section 83 of the TIA Act
- particulars of any deficiencies identified that impact on the integrity of the telecommunications interception regime, and
- particulars of any remedial action taken or proposed to be taken to address those deficiencies.

4.76 The Ombudsman completed two inspections each of the ACC's and AFP's records during the reporting period. The reports concluded that both agencies demonstrate a high degree of compliance with the detailed record keeping requirements of the TIA Act.

The ACC

4.77 The Ombudsman found the ACC to be compliant with the requirements of the TIA Act for the keeping of records connected with the issue of warrants (section 80) and other records in connection with interceptions (section 81). The Ombudsman also found the ACC to be generally compliant with the requirements relating to the destruction of records (section 79). The Ombudsman did note that in some instances the ACC destroyed restricted records without the prior approval of the CEO. However, the CEO was made aware of this oversight prior to the inspection and subsequently granted approval for the destruction.

4.78 The Ombudsman commented on the ACC's cooperative approach towards inspections, and noted that the ACC's Electronic Product Management Centre seeks to continuously improve its administrative processes and procedures. The Ombudsman did not make any recommendation as a result of either inspection of the ACC.

The AFP

4.79 The Ombudsman found the AFP to be compliant with all the requirements of the Act, being for the keeping of records connected with the issue of warrants (section 80) and other records in connection with interceptions (section 81) and with the requirements relating to the destruction of records (section 79).

4.80 The Ombudsman noted that in some cases the AFP's use and communications logs did not identify some communications of lawfully intercepted information to other enforcement and security agencies and the Commonwealth Director of Public Prosecutors, and did not maintain sufficient detail in relation to some internal communications. Accordingly, the Ombudsman recommended that the AFP should ensure that its use and communications logs are accurate and sufficiently detailed.

4.81 The AFP has advised that internal procedures have been put in place to monitor and address the issue.

Other information

4.82 Paragraph 103(b) of the TIA Act provides that the report must set out such other information (if any) as is prescribed. There was no other information prescribed during the reporting period.

Stored communications

4.83 The Ombudsman also inspected the records of 14 enforcement agencies pursuant to the stored communications provisions of the TIA Act and provided the reports to the Department under section 153(1) of the TIA Act. The agencies inspected were the AFP, the Australian Crime Commission (ACC), the Australian Securities and Investments Commission, Australian Customs and Border Protection Service, the NSW Crime Commission, NSW Police, the Victorian Office of Police Integrity, Queensland Police, South Australia Police, Tasmania Police, Victoria Police, Western Australia Police, the Corruption and Crime Commission (Western Australia).

4.84 The Ombudsman found that all enforcement agencies were compliant or generally compliant with the record keeping requirements relating to the issue of stored communications warrants under section 151 of the TIA Act.

Period of warrant

4.85 The Ombudsman identified a systemic issue with agencies receiving information from carriers that did not contain enough information to determine whether stored communications were accessed within the period of the warrant. Agencies and the Attorney-General's Department are working with industry to achieve best practice by ensuring agencies get enough information to enable them to determine whether the information has been lawfully accessed at an early stage in investigations.

4.86 There were a small number of instances where stored communications were identified as not having been accessed within the parameters of warrants. In these circumstances, agencies have quarantined the information from further use by investigators. Agencies have either destroyed or advised that they will destroy quarantined information in accordance with the TIA Act requirements.

Subject of warrant

4.87 The Ombudsman identified circumstances were it appeared stored communications warrants were obtained over persons not involved in the offence as required by the TIA Act. In these circumstances, agencies reviewed their application procedures and have quarantined the information for destruction.

Issuing authorities

4.88 The Ombudsman identified a small number of stored communications warrants which had been signed by issuing authorities whose powers did not extend to this role. The Department has provided agencies with updated information relating the current status of issuing authorities.

CHAPTER 5—STORED COMMUNICATIONS INFORMATION REQUIRED UNDER THE ACT

The information required

5.1 The reporting requirements of the TIA Act in relation to accessing stored communications are contained in Part 3-6 of the TIA Act, which provides that this report must include information on:

- the relevant statistics relating to applications for stored communication warrants that were made by the agency during the reporting period (paragraph 162(2)(a))
- the relevant statistics relating to telephone applications for stored communication warrants made by the agency during the reporting period (paragraph 162(2)(b))
- the relevant statistics relating to renewal warrants that were made by the agency during the reporting period (paragraph 162(2)(c))
- the number of warrants which were issued with specified conditions or restrictions (paragraph 162(2)(d))
- the number of arrests made during the reporting period based on lawfully intercepted information (paragraph 163(a)), and
- the number of proceedings which ended in the reporting period in which information collected by means of a warrant was given in evidence (paragraph 163(b)).

5.2 The TIA Act provides that the information must be set out in relation to each agency that is entitled to be issued with warrants authorising access to stored communications. In addition, the information must be combined for all agencies to indicate the overall extent and effectiveness of access to stored communications under the TIA Act.

5.3 It is possible for an enforcement agency to record arrests, proceedings in which lawfully accessed information was given in evidence or convictions based on lawfully accessed information where the agency has not applied for stored communications warrants. This can arise where an agency has received stored communications for purposes provided for by section 139 of the TIA Act but was not the agency that applied for the warrant.

Which agencies may seek stored communications warrants?

5.4 Any enforcement agency may apply for a stored communications warrant. The definition of enforcement agency includes criminal law enforcement agencies, civil penalty enforcement agencies or public revenue agencies. This includes all the bodies mentioned as interception agencies and eligible authorities for the purposes of telecommunications interception warrants, as well as other regulatory bodies such as the:

- Australian Customs and Boarder Protection Service
- the Australian Securities and Investments Commission
- the Australian Competition and Consumer Commission
- the Australian Taxation Office, and
- Centrelink.

Applications for stored communications warrants

5.5 Paragraphs 162(1)(a) and (2)(a) of the TIA Act provide that the report must set out how many applications for stored communications warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting year for each agency and in total. This information is presented in Table 52. Only those enforcement agencies that applied for stored communications warrants during the reporting period are included in the table.

5.6 There was a 7% decrease in the use of stored communications warrants in the reporting period. This is in line with operational priorities which regularly reflect small increases and decreases from reporting period to reporting period.

Table 52—Applications for stored communications warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		07/08	08/09	09/10
ACC	Made Refused/withdrawn Issued	12 - 12	8 - 8	55 - 55
AFP	Made Refused/withdrawn Issued	13 - 13	41 - 41	39 - 39
ASIC	Made Refused/withdrawn Issued	1 - 1	6 - 6	10 - 10
CCC WA	Made Refused/withdrawn Issued	- - -	4 - 4	1 - 1
CMC	Made Refused/withdrawn Issued	- - -	29 1 28	23 - 23
CUSTOMS	Made Refused/withdrawn Issued	1 - 1	9 - 9	7 - 7
NSW CC	Made Refused/withdrawn Issued	1 - 1	6 - 6	1 - 1
NSW POLICE	Made Refused/withdrawn Issued	27 - 27	26 - 26	22 - 22
NT POLICE	Made Refused/withdrawn Issued	6 - 6	- - -	2 - 2
OPI	Made Refused/withdrawn Issued	- - -	12 - 12	2 - 2
PIC	Made Refused/withdrawn Issued	3 - 3	- - -	- - -
QLD POLICE	Made Refused/withdrawn Issued	27 - 27	119 - 119	66 - 66
SA POLICE	Made Refused/withdrawn Issued	1 - 1	8 - 8	5 - 5
TAS POLICE	Made Refused/withdrawn Issued	8 - 8	36 - 36	46 - 46
VIC POLICE	Made Refused/withdrawn Issued	5 - 5	9 - 9	6 - 6
WA POLICE	Made Refused/withdrawn Issued	12 - 12	8 - 8	14 - 14
TOTAL [paragraph 162(2)(a)]	**Made** **Refused/withdrawn** **Issued**	**117** **-** **117**	**321** **1** **320**	**299** **-** **299**

Telephone applications for stored communications warrants

5.7 Paragraphs 162(1)(b) and (2)(b) of the TIA Act provide that the report must set out how many telephone applications for stored communications warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting period for each agency and in total. This information is presented in Table 53.

Table 53—Telephone applications for stored communications warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		07/08	08/09	09/10
NSW POLICE	Made	-	1	3
	Refused/withdrawn	-	-	-
	Issued	-	1	3
VIC POLICE	Made	-	-	2
	Refused/withdrawn	-	-	-
	Issued	-	-	2
TOTAL	Made	-	1	5
	Refused/withdrawn	-	-	-
	Issued	-	1	5

Renewal applications for stored communications warrants

5.8 Paragraph 162(2)(c) of the TIA Act provides that the report must set out how many renewal applications for stored communications warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting period for each agency and in total. This information is presented in Table 54.

Table 54—Renewal applications for stored communications warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		07/08	08/09	09/10
CMC	Made	-	15	-
	Refused/withdrawn	-	-	-
	Issued	-	15	-

Stored communications warrants subject to conditions or restrictions

5.9 Paragraph 162(2)(d) of the TIA Act provides that the report must set out how many stored communications warrants issued on application made during the reporting period specified conditions or restrictions, for each agency and in total. This information is presented in Table 55.

Table 55—Stored communications warrants subject to conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		07/08	08/09	09/10
AFP	Made	-	-	1
	Refused/withdrawn	-	-	-
	Issued	-	-	1
QLD POLICE	Made	-	20	1
	Refused/withdrawn	-	-	-
	Issued	-	20	1
TOTAL	Made	-	20	2
	Refused/withdrawn	-	-	-
	Issued	-	20	2

Effectiveness of stored communications warrants

The number of arrests, proceedings and convictions made during the reporting period based on lawfully accessed information

5.10 Section 163 of the TIA Act provides that the report must set out the number of arrests made on the basis of lawfully accessed information and the number of proceedings in which lawfully accessed information was given in evidence. This information is set out in Table 56. The table also includes the number of convictions recorded based on lawfully accessed information.

Table 56—Number of arrests, proceedings and convictions made on the basis of lawfully accessed information

AGENCY	ARRESTS			PROCEEDINGS			CONVICTIONS		
	07/08	08/09	09/10	07/08	08/09	09/10	07/08	08/09	09/10
ACC	**-**	**-**	10	**-**	**-**	**-**	**-**	**-**	**-**
AFP	-	27	1	-	5	1	-	-	-
CMC	-	-	15	-	-	-	-	-	-
CUSTOMS	-	-	3	-	-	1	-	-	-
NSW CC	-	-	-	-	-	-	-	-	-
NSW POLICE	7	21	10	1	24	22	1	19	20
NT POLICE	-	-	1	-	-	-	-	-	-
QLD POLICE	36	69	47	-	1	12	-	1	12
SA POLICE	-	-	-	-	-	2	-	-	2
TAS POLICE	-	10	25	-	2	7	-	-	8
VIC POLICE	3	8	1	-	-	3	-	-	7
WA POLICE	-	4	-	-	-	-	-	-	-
TOTAL	**46**	**139**	**113**	**1**	**32**	**48**	**1**	**20**	**49**

Interpretative note relating to prosecutions and convictions statistics

5.11 It should be noted that stored communications warrants will usually authorise access to less information than can be obtained under a telecommunications interception warrant, meaning that multiple stored communications warrants may often be obtained as part of a single investigation.

5.12 Additionally, the information in Table 56 should be interpreted with caution. Due to operational priorities, an arrest recorded in one reporting period may not result in a prosecution/committal (if at all) until a later reporting period and any resulting conviction may be recorded in that or an even later reporting period. Additionally, the number of arrests may not equate to the number of charges laid as an arrested person may be prosecuted and convicted for a number of offences, some or all of which may be prosecuted at a later time.

CHAPTER 6—TELECOMMUNICATIONS DATA - INFORMATION REQUIRED UNDER THE ACT

The information required

6.1 The reporting requirements of the TIA Act in relation to authorising the disclosure of telecommunications data are contained in Part 4-2 of the TIA Act. Part 4-2 provides that this report must include information on:

- the number of authorisations made under section 178 (paragraph 186(1)(a))
- the number of authorisations made under section 179 (paragraph 186(1)(b))
- for criminal law-enforcement agencies – the number of authorisations made under section 180 (paragraph 186(1)(c)), and
- any other matter requested by the Minister in relation to those authorisations (paragraph 186(1)(d)).

Which agencies may authorise the disclosure of telecommunications data

6.2 Agencies are able to authorise the disclosure of telecommunications data if they are an enforcement agency. An enforcement agency is an agency responsible for the administration of a legislation which enables them to enforce a criminal law, impose pecuniary penalties or protect the public revenue.

6.3 An authorised officer of an enforcement agency is able to make the authorisation. An authorised officer means the head, deputy head, or a person who holds an office or position covered by an authorisation under subsection 5AB(1) of the TIA Act. Enforcement agencies notify the Communications Access Co-ordinator of the positions which can authorise the disclosure of telecommunications data.

Authorisations granted

6.4 The telecommunications data regime was transferred to the TIA Act on 1 November 2007. Therefore, statistics were sought from agencies for authorisations made from that date. The 2007-2008 statistics are lower than the 2008-2009 and 2009-2010 reporting periods, because figures were only reported for part of the 2007-2008 reporting period.

6.5 The number of authorisations made for access to existing information or documents in the enforcement of the criminal law is given at Table 57. The number of authorisations made for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue is given in Table 58.

Table 57—Number of authorisations made for access to existing information or documents in the enforcement of the criminal law

AGENCY	AUTHORISATIONS		
	07/08	08/09	09/10
ACC	5,639	9,038	12,467
ACLEI	5	28	65
AFP	12,996	16,942	20,869
AUSTRALIAN COMPETITION & CONSUMER COMMISSION	2	7	35
AUSTRALIAN FISHERIES MANAGEMENT AUTHORITY	-	-	2
AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION	1,076	2,319	2,874
AUSTRALIAN TAXATION OFFICE	17	644	610
CCC WA	265	394	506
CMC	5,716	9,468	1,516
CUSTOMS	2,022	9,040	4,157
DEPARTMENT OF AGRICULTURE, FISHERIES AND FORESTRY	3	110	89
DEPARTMENT OF COMMERCE (WA)	217	152	184
DEPARTMENT OF CORRECTIVE SERVICES (NSW)	-	-	37
DEPARTMENT OF DEFENCE	13	48	30
DEPARTMENT OF ENVIRONMENT AND CLIMATE CHANGE NSW	19	60	119
DEPARTMENT OF ENVIRNOMENT, WATER, HERITAGE AND THE ARTS	-	-	22
DEPARTMENT OF FAMILIES, HOUSING, COMMUNITY SERVICES AND INDIGENOUS AFFAIRS	-	22	7
DEPARTMENT OF IMMIGRATION AND CITIZENSHIP	-	-	86
DEPARTMENT OF JUVENILE JUSTICE (NSW)	-	1	-
DEPARTMENT OF PRIMARY INDUSTRIES (VIC)	191	421	464
DEPARTMENT OF TRANSPORT (VICTORIAN TAXI DIRECTORATE)	-	-	3
ICAC	199	260	450
INSOLVENCY AND TRUSTEE SERVICE AUSTRALIA	-	-	211
NSW CC	3,011	4,620	3,602
NSW POLICE	88,368	100,585	115,343
NT POLICE	979	807	1,834

AGENCY	AUTHORISATIONS		
	07/08	08/09	09/10
OPI	1,001	873	2,235
PIC	2,048	1,815	1,242
QLD POLICE	4,529	9,344	10,223
ROYAL SOCIETY FOR THE PREVENTION OF CRUELTY TO ANIMALS (QLD)	2	-	46
ROYAL SOCIETY FOR THE PREVENTION OF CRUELTY TO ANIMALS (VIC)	8	7	16
SA POLICE	7,852	3,442	11,631
TAS POLICE	-	9,627	6,689
TRANSPORT ACCIDENT COMMISSION (VIC)	3	-	2
VIC POLICE	46,643	40,617	50,234
WA POLICE	275	24,606	26,234
TOTAL	**183,099**	**245,297**	**274,134**

Table 58—Number of authorisations made for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue

AGENCY	AUTHORISATIONS		
	07/08	08/09	09/10
ACLEI	-	4	-
ACT REVENUE OFFICE	7	5	-
AFP	481	549	267
AUSTRALIAN BUILDING AND CONSTRUCTION COMMISSION	13	14	12
AUSTRALIAN COMPETITION AND CONSUMER COMMISSION	29	-	10
AUSTRALIAN FISHERIES MANAGEMENT AUTHORITY	-	7	4
AUSTRALIA POST	229	298	361
AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION	111	148	123
AUSTRALIAN TAXATION OFFICE	1,407	645	504
CENTRELINK	2	1,926	2579
CHILD SUPPORT AGENCY	532	192	74
CONSUMER AFFAIRS AND FAIR TRADING (TAS)	3	-	-
CONSUMER AFFAIRS (VIC)	328	441	235

CORRECTIONS VICTORIA	-	-	52
CMC	-	-	1
CUSTOMS	1,526	1,096	225
DEPARTMENT OF AGRICULTURE, FISHERIES AND FORESTRY	22	6	-
DEPARTMENT OF COMMERCE (NSW) - OFFICE OF FAIR TRADING	439	658	1,012
DEPARTMENT OF COMMERCE (WA)	-	-	20
DEPARTMENT OF CONSUMER AND EMPLOYMENT PROTECTION (WA)	10	-	-
DEPARTMENT OF DEFENCE	44	1	8
DEPARTMENT OF EMPLOYMENT, ECONOMIC DEVELOPMENT AND INNOVATION (QLD)	-	4	21
DEPARTMENT OF ENVIRNOMENT AND CONSERVATION (WA)	-	-	18
DEPARTMENT OF ENVIRONMENT AND RESOURCE MANAGEMENT (QLD)	-	-	3
DEPARTMENT OF FAMILIES, HOUSING, COMMUNITY SERVICES AND INDIGENOUS AFFAIRS	-	1	-
DEPARTMENT OF HUMAN SERVICES – JUVENILE JUSTICE (NSW)	-	-	1
DEPARTMENT OF IMMIGRATION AND CITIZENSHIP	-	-	204
DEPARTMENT OF JUSTICE NT (FORMERLY DEPARTMENT OF JUSTICE AND CONSUMER AFFAIRS (NT)	-	-	2
DEPARTMENT OF PRIMARY INDUSTRIES (VIC)	-	-	1
DEPARTMENT OF SUSTAINABILITY AND ENVIRONMENT (VIC)	105	11	75
DEPARTMENT OF TRANSPORT (VICTORIAN TAXI DIRECTORATE)	-	-	3
DEPARTMENT OF TREASURY (QLD)	-	-	27
HEALTH CARE COMPLAINTS COMMISSION (NSW)	1	2	8
ICAC	82	227	24
DEPARTMENT OF INDUSTRY AND INVESTMENT (NSW)	33	81	108
NT POLICE	14	-	-
OFFICE OF CONSUMER AND BUSINESS AFFAIRS (SA)	51	124	201
OFFICE OF STATE REVENUE (NSW)	-	132	132
OFFICE OF STATE REVENUE (QLD)	1	53	27

ENVIRONMENTAL PROTECTION AGENCY (QLD) [12]	15	50	-
QLD POLICE	1	-	-
REVENUE SA	53	36	77
STATE REVENUE OFFICE (VIC)	68	103	130
TAS POLICE	-	189	-
TASMANIAN PRISON SERVICE	-	8	3
TERRITORY REVENUE OFFICE (NT)	1	1	-
WORKCOVER (QLD)	41	6	4
WORKSAFE (VIC)	-	-	27
TOTAL	**5,649**	**7,014**	**6,583**

6.6 The number of authorisations made by a criminal law-enforcement agency for access to specified information or documents that come into existence during the period for which the authorisations is in force is given in Table 59. The table also outlines the number of days the authorisations were specified in force, and for how many days they were in force. The number of authorisations still in force at the end of the reporting period is also given.

[12] Now captured under Department of Environment and Resource Management

AGENCY	NUMBER OF AUTHORISATIONS MADE			DAYS SPECIFIED IN FORCE			ACTUAL DAYS IN FORCE			AUTHORISATIONS DISCOUNTED		
	07/08	08/09	09/10	07/08	08/09	09/10	07/08	08/09	09/10	07/08	08/09	09/10
ACC	37	42	114	1,481	1,459	4,461	1,019	1,031	2,884	2	2	-
AFP	68	103	148	2,164	3,152	4,577	927	2,879	3,714	8	12	7
CCC WA	-	49	67	-	1,069	2,502	-	1,098	1,840	-	16	6
CMC	11	129	174	44	1,554	6,927	44	1,466	6,919	-	9	20
CUSTOMS	-	-	3	-	-	46	-	-	46	-	-	-
ICAC	-	-	2	-	-	3	-	-	3	-	-	-
NSW CC	330	720	967	6,590	16,612	27,078	4,959	12,539	24,740	29	61	64
NSW POLICE	196	237	221	5,452	5,027	5,771	3,220	3,908	3,960	11	10	10
NT POLICE	81	356	322	3,577	16,020	14,448	2,955	14,507	12,234	26	-	20
OPI	54	75	16	2,147	4,299	719	1,824	3,146	561	1	8	9
PIC	79	106	127	2,994	3,466	5,299	1,966	4,143	4,218	20	3	25
QLD POLICE	61	192	451	1,326	3,109	9,775	867	2,164	8,684	10	15	41
SA POLICE	45	53	83	1,290	1,560	2,953	723	1,078	1,755	1	4	6
TAS POLICE	26	65	40	985	2,771	1,800	455	1,660	1,007	-	1	-
VIC POLICE	214	211	797	4,896	7,614	25,335	2,500	4,887	18,357	11	11	32
WA POLICE	113	233	272	4,747	8,808	12,270	1,778	4,463	11,496	4	18	33
TOTAL	**1,315**	**2,571**	**3,804**	**37,693**	**77,060**	**123,964**	**23,237**	**58,969**	**102,418**	**123**	**170**	**273**

6.7 Information is also given about the average number of days the authorisations were specified in force, and the average actual number of days they remained in force. This information is presented at Table 60.

Table 60—Average specified and actual time in force

AGENCY	AVERAGE PERIOD SPECIFIED			AVERAGE PERIOD ACTUAL		
	07/08	08/09	09/10	07/08	08/09	09/10
ACC	40	35	39	29	26	25
AFP	32	31	31	15	32	26
CCC WA	-	33	37	-	32	30
CMC	4	12	40	4	12	45
CUSTOMS	-	-	15	-	-	15
ICAC	-	-	2	-	-	2
NSW CC	20	23	28	16	19	27
NSW POLICE	28	21	26	17	17	19
NT POLICE	44	45	45	54	41	41
OPI	40	57	45	34	47	80
PIC	38	33	42	33	40	41
QLD POLICE	22	16	22	17	12	21
SA POLICE	29	29	36	16	22	23
TAS POLICE	38	43	45	18	26	25
VIC POLICE	23	36	32	12	24	24
WA POLICE	42	38	45	16	21	48
TOTAL	**29**	**30**	**33**	**19**	**23**	**31**