Office of the Inspector
of the Independent Commission
Against Corruption

Report of an audit of applications for and execution of Surveillance Device Warrants and Retrieval Warrants by the Independent Commission Against Corruption

May 2012

by

The Inspector of the
Independent Commission Against Corruption

CONTENTS

1. THE PURPOSE OF THE AUDIT

From time to time, as part of its investigations into alleged serious and systemic corrupt conduct, the Independent Commission Against Corruption (the ICAC or the Commission) obtains surveillance device warrants pursuant to the *Surveillance Devices Act 2007* (the SD Act).

The present audit examines the Commission's applications for and execution of all Surveillance Device Warrants and Retrieval Warrants pursuant to Part 3 of the SD Act during the year 2011.

Section 4 of the SD Act contains the following definitions:

> "Surveillance device" means:
>
> (a) a data surveillance device, a listening device, an optical surveillance device or a tracking device, or
> (b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a), or
> (c) a device of a kind prescribed by the regulations.
>
> "Data surveillance device" means:
>
> any device or program capable of being used to record or monitor the input of information into or output of information from a computer, but does not include an optical surveillance device.
>
> "Optical surveillance device" means:
>
> any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.
>
> "Tracking device" means:
>
> any electronic device capable of being used to determine or monitor the geographical location of a person or an object.

The use of such surveillance devices to monitor a person's computer and/or to observe and monitor a person's movements and to record such observations without the knowledge of that person is a serious intrusion into the right of privacy of that person.

In addition, such use is a covert activity the presence of which is an unknown to that person. Consequently, he/she is not in a position to raise a complaint or protest.

On the other hand, there are circumstances in which the covert use of surveillance devices can provide evidence which can facilitate the detection and/or prevention of a serious crime or aid the prosecution of a person or persons involved in serious criminal activity.

The SD Act after prohibiting the use of surveillance devices and the publication of the fruits of such use goes on to authorise the ICAC covertly to use such devices in limited circumstances.

The purpose of this audit is to examine a sample of cases in which the ICAC has used such surveillance devices:

- to determine whether it has obeyed the terms of the legislation.
- to examine the systems instituted and maintained by the ICAC to ensure such use is limited to those circumstances where it is lawful and appropriate for the conduct of its statutory functions.

2. THE INSPECTOR'S AUDIT FUNCTION

Section 57B(1)(a) of the *Independent Commission Against Corruption Act 1988* (the ICAC Act or the Act) authorises the Inspector of the Independent Commission Against Corruption (the Inspector) to audit the operations of the ICAC for the purpose of monitoring compliance with the law of the State.

The Inspector's audit role must be read in the context of the Inspector's other functions prescribed under section 57B, namely section 57B(1)(c) and (d). Section 57B(1)(c) of the ICAC Act authorises the Inspector to deal with (by reports and recommendations) conduct amounting to maladministration (including, without limitation, delay in the conduct of investigations and unreasonable invasions of privacy) by the Commission or officers of the Commission.

Section 57B(1)(d) of the ICAC Act authorises the Inspector to assess the effectiveness and appropriateness of the procedures of the Commission relating to the legality and propriety of its activities.

Section 57B(2) states that the functions of the Inspector may be exercised on the Inspector's own initiative.

3. THE AMBIT OF THE AUDIT

Pursuant to section 57B of the *Independent Commission Against Corruption Act 1988* (the ICAC Act), I have audited and assessed the effectiveness and appropriateness of the procedures of the Commission in relation to the application for and execution of the Surveillance Device Warrants and Retrieval Warrants pursuant to Part 3 of the *Surveillance Devices Act 2007* (the SD Act) during the year 2011.

The audit and assessment examined:

1. the Commission's compliance with the formal and procedural requirements under the SD Act;
2. the reasons behind the Commission's decision to apply for such warrants;
3. the manner in which the Commission executed the warrants; and
4. any other matters set out in section 57B of the ICAC Act.

For the purposes of this exercise I have reviewed the Commission's files and records relating to all applications for Surveillance Device Warrants and Retrieval Warrants pursuant to Part 3 of the SD Act during the year 2011, regardless of whether they were granted or refused by an eligible judge or magistrate.

The Commission advised that six applications for Surveillance Device Warrants were sought and granted during the nominated period, that no applications for a Surveillance Device Warrant were refused and that no applications were made for a Retrieval Warrant.

At the time of my last audit of the Commission's use of surveillance devices in April 2011, the Commissioner contended (in my view correctly) that the provisions of the SD Act prima facie, prohibited him from furnishing "protected information" to the Inspector for the purpose of an audit (as opposed to the purpose of a targeted inquiry). At that time, applying sections 40(6) and 40(7) of the Act as it then was, he determined that it was in the public interest to

provide the information and, therefore, did so. This means that the Inspector's power to conduct an audit of the use of any surveillance device was dependent upon the willingness of the Commissioner to make a determination that it is in the public interest to provide the information.

In that report I recommended appropriate statutory amendments to overcome the need for the Commissioner to make such a determination.

Such amendments were made to the ICAC Act by the *Independent Commission Against Corruption Amendment Act 2011 No 36* which inserted at the end of section 57F:

> (2) Section 40 of the *Surveillance Devices Act 2007* does not apply to the use, publication or communication of protected information within the meaning of that Act in relation to the exercise of the Inspector's functions under section 57B.

The amending Act of 2011 inserted Part 11 into the ICAC Act, clause 31 of which states:

> The amendment made to section 57F by the amending Act extends to the use, publication or communication before the commencement of the amendment of protected information within the meaning of the Surveillance Devices Act 2007 in relation to the exercise of the Inspector's functions under section 57B.

Accordingly my audit powers in relation to Surveillance Devices are no longer dependent upon the willingness of the Commissioner to make a determination that disclosure of the information is in the public interest.

4. THE RELEVANT PROVISIONS OF THE SURVEILLANCE DEVICES ACT

The relevant definitions in section 4 of the SD Act have been set out above.

Section 8 of the SD Act provides:

1) A person must not knowingly install, use or maintain an optical surveillance device on or within premises or a vehicle or on any other object, to record visually or observe the carrying on of an activity if the installation, use or maintenance of the device involves:

   (a) entry onto or into the premises or vehicle without the express or implied consent of the owner or occupier of the premises or vehicle, or

   (b) interference with the vehicle or other object without the express or implied consent of the person having lawful possession or lawful control of the vehicle or object.

   Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

This prohibition does not apply to the installation, use or maintenance of an optical surveillance device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation.

Section 9 of the SD Act provides:

1) A person must not knowingly install, use or maintain a tracking device to determine the geographical location of:

   (a) a person—without the express or implied consent of that person, or

   (b) an object—without the express or implied consent of a person in lawful possession or having lawful control of that object.

   Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

This prohibition does not apply to the installation, use or maintenance of a tracking device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation.

Section 10 of the SD Act provides:

1) A person must not knowingly install, use or maintain a data surveillance device on or in premises to record or monitor the input of information into, or the output of information from, a computer on the premises if the installation, use or maintenance of the device involves:

   (a) entry onto or into the premises without the express or implied consent of the owner or occupier of the premises, or

   (b) interference with the computer or a computer network on the premises without the express or implied consent of the person having lawful possession or lawful control of the computer or computer network.

   Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

This prohibition does not apply to the installation, use or maintenance of a data surveillance device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation.

Section 11 prohibits a person from publishing or communicating to any person, a private conversation or a record of the carrying on of an activity, or a report of a private conversation or carrying on of an activity, that has come to the person's knowledge as a direct or indirect result of the use of a listening device, an optical surveillance device or a tracking device in contravention of a provision of this Part and section 12 prohibits the possession of a record of private conversation or activity.

Section 14 prohibits a person from publishing or communicating to any person, any information regarding the input of information into, or the output of information from, a computer obtained as a direct or indirect result of the use of a data surveillance device in contravention of this Part.

The method and grounds of an application for such a warrant are set out in section 17 of the SD Act in these terms:

1) A law enforcement officer (or another person on his or her behalf) may apply for the issue of a surveillance device warrant if the law enforcement officer on reasonable grounds suspects or believes that:

   (a) a relevant offence has been, is being, is about to be or is likely to be committed, and

   (b) an investigation into that offence is being, will be or is likely to be conducted in this jurisdiction or in this jurisdiction and in one or more participating jurisdictions, and

   (c) the use of a surveillance device is necessary for the purpose of an investigation into that offence to enable evidence to be obtained of the commission of that offence or the identity or location of the offender.

2) The application may be made to:

   (a) an eligible Judge in any case, or

   (b) an eligible Magistrate in the case of an application for a surveillance device warrant authorising the use of a tracking device only.

3) An application:

   (a) must specify:

      i. the name of the applicant, and
      ii. the nature and duration of the warrant sought, including the kind of surveillance device sought to be authorised, and

   (b) subject to this section, must be supported by an affidavit setting out the grounds on which the warrant is sought.

4) If a law enforcement officer believes that:

   (a) the immediate use of a surveillance device is necessary for a purpose referred to in subsection (1)(c), and

   (b) it is impracticable for an affidavit to be sworn before an application for a warrant is made, an application for a warrant may be made before an affidavit is prepared or sworn.

5) If subsection (4) applies, the applicant must:

   (a) provide as much information as the eligible Judge or eligible Magistrate considers is reasonably practicable in the circumstances, and

(b) not later than 72 hours following the making of the application, send a duly sworn affidavit to the eligible Judge or eligible Magistrate, whether or not a warrant has been issued.

6) An application for a warrant is not to be heard in open court.

Section 19 sets out the matters upon which the eligible judge must be satisfied, namely:

1) An eligible Judge or eligible Magistrate may issue a surveillance device warrant if satisfied:

   (a) that there are reasonable grounds for the suspicion or belief founding the application for the warrant, and

2) In determining whether a surveillance device warrant should be issued the eligible Judge or eligible Magistrate must have regard to:

   (a) the nature and gravity of the alleged offence in respect of which the warrant is sought, and

   (b) the extent to which the privacy of any person is likely to be affected, and

   (c) the existence of any alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation, and

   (d) the extent to which the information sought to be obtained would assist the investigation, and

   (e) the evidentiary value of any information sought to be obtained, and

   (f) any previous warrant sought or issued under this Part or a corresponding law (if known) in connection with the same offence.

The term "law enforcement agency" includes the Independent Commission Against Corruption, and "law enforcement officer" means, in relation to the Independent Commission Against Corruption—an officer of the Commission within the meaning of the *Independent Commission Against Corruption Act 1988.*

The contents of such a warrant are prescribed by section 20:

1) A surveillance device warrant must:

   (a) state that the eligible Judge or eligible Magistrate is satisfied of the matters referred to in section 19(1) and has had regard to the matters referred to in section 19(2), and

   (b) specify:

      (i) the name of the applicant, and

      (ii) the alleged offence in respect of which the warrant is issued, and

      (iii) the date the warrant is issued, and

      (iv) the kind of surveillance device authorised to be used, and

      (v) if the warrant authorises the use of a surveillance device on or in premises or a vehicle—the premises or vehicle on or in which the use of the surveillance device is authorised, and

      (vi) if the warrant authorises the use of a surveillance device in or on an object or class of object—the object or class of object in or on which the use of the surveillance device is authorised, and

      (vii) if the warrant authorises the use of a surveillance device on or about the body of a person—the name of the person, and

      (viii) if the warrant authorises the use of a surveillance device in respect of the conversations, activities or geographical location of a person—the name of the person (if known), and

      (ix) the period during which the warrant is in force, being a period not exceeding 90 days, and

      (x) the name of the law enforcement officer primarily responsible for executing the warrant, and

      (xi) any conditions subject to which premises or vehicle may be entered, or a surveillance device used, under the warrant.

2) In the case of a warrant referred to in subsection (1)(b)(vii), if the identity of the person is unknown, the warrant must state that fact.

3) A warrant must be signed by the eligible Judge or eligible Magistrate issuing it and include his or her name.

4) If an eligible Judge or eligible Magistrate issues a warrant on a remote application:

(a) the eligible Judge or eligible Magistrate must inform the applicant of:

(i) the terms of the warrant, and

(ii) the date on which and the time at which the warrant was issued, and cause those details to be entered in a register kept by the Judge or Magistrate for that purpose, and

(b) the Judge or Magistrate must provide the applicant with a copy of the warrant as soon as possible.

Under section 44(1) of the SD Act:

1) A person to whom a surveillance device warrant is issued must, within the time specified in the warrant, furnish a report, in writing, to an eligible Judge (if the warrant was issued by an eligible Judge) or eligible Magistrate (if the warrant was issued by an eligible Magistrate) and to the Attorney General:

(a) stating whether or not a surveillance device was used pursuant to the warrant, and

(b) specifying the type of surveillance device (if any) used, and

(c) specifying the name, if known, of any person whose private conversation was recorded or listened to, or whose activity was recorded, by the use of the device, and

(d) specifying the period during which the device was used, and

(e) containing particulars of any premises or vehicle on or in which the device was installed or any place at which the device was used, and

(f) containing particulars of the general use made or to be made of any evidence or information obtained by the use of the device, and

(g) containing particulars of any previous use of a surveillance device in connection with the relevant offence in respect of which the warrant was issued.

Section 51(1) of the SD Act provides that particulars of warrants sought must be notified to Attorney General, whilst subsection (2) sets out the matters as to which the eligible Judge or eligible Magistrate is to be satisfied before issuing the warrant.

5. ICAC'S SYSTEMS TO CONTROL AND REGULATE THE APPLICATION FOR AND USE OF SURVEILLANCE DEVICE WARRANTS

The Commission's Operations Manual contains two procedures regarding surveillance device warrants. The first is Procedure 10A entitled "Procedures for Obtaining and Executing Surveillance Device Warrants". The second is Procedure 10B entitled "Procedures for Use and Recording Surveillance Devices Act Information". Both were approved on 10 April 2008. The former was amended on 19 August 2008 and reviewed on 23 November 2010. The latter was reviewed on 20 May 2010.

Procedure 10A contains general information regarding the definition of surveillance devices, sets out the circumstances when a warrant is required and the process for obtaining such a warrant. It specifies that in all cases the following steps will be followed:

1. The Case Officer will discuss with the Case Lawyer (if there is no Case Lawyer the Executive Director, Legal will assign one) to determine whether or not a warrant is required for the proposed use of a surveillance device or devices.
2. The Case Officer will obtain the approval of the Executive Director, ID to make an application. The approval is to be recorded on the Authorisation Checklist a form of which is at Appendix A of the Procedure.
3. If approval is given for an application the Case Officer (includes nominated Lead Investigator) will notify the Chief Investigator, Surveillance and Technical Unit (STU), by e-mail outlining the requested tasking, investigation objectives, timings, potential risks, numbers and types of surveillance devices likely to be required and whether any are to be installed on persons, premises, objects or vehicles. The e-mail is to be copied to the Case Lawyer.
4. Where it is proposed to install a surveillance device on the premises, an object or a vehicle the Executive Director, ID, will decide whether the STU

should be responsible for the installation or whether an outside agency will be asked to assist.

5. Once the Executive Director, ID has given approval for the use of the surveillance device(s) the Case Officer will obtain the sequential warrant number from the Chief Investigator, STU.

5 [Sic]. The Case Officer will advise the Case Lawyer of approval and, using the approved pro forma, prepare the affidavit in support of the application, the application and the warrant.

6. The Case Officer will ensure that the affidavits:
   - discloses all relevant material facts, and
   - addresses the following matters under section 19(2) of the SD Act, being the matters which must be considered by the judge/magistrate:

   (a) The nature and gravity of the alleged offence in respect of which the warrant is sought;
   (b) The extent to which the privacy of any person is likely to be affected;
   (c) The existence of any alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation;
   (d) The extent to which the information sought to be obtained would assist the investigation;
   (e) The evidentiary value of any evidence sought to be obtained; and
   (f) Any previous warrant sought or granted under the SD Act or corresponding law (if known) in connection with the same offence.

7. Once prepared the Case Officer will submit the draft documents to the Case Officer's Chief Investigator for checking for factual accuracy.
8. The Chief Investigator will submit the draft documents and the Authorisation Checklists to the Case Lawyer.
9. The Case Lawyer is responsible for preparing:
   (a) the notification to the Attorney General under section 51 of the SD Act.
   (b) the affidavit deposing to the service of the section 51 notification.

10. The Case Lawyer will ensure that:
    (a) all documentation meets the requirements of the SD Act; and
    (b) sufficient grounds are made out in the affidavit to support the application.
11. Once settled by the Case Lawyer the draft documentation is to be referred to the Executive Director, Legal, for approval. Approval is to be recorded on the Authorisation Checklist.
12. Once the application is approved by the Executive Director, Legal the Case Lawyer is responsible for arranging service of the section 51 notification.
13. Once approved, the Case Lawyer will arrange for the application to be signed and the affidavit sworn by the Case Officer who is the law enforcement officer for the purpose of the application.
14. Once the Solicitor General has responded to the section 51 notification the Case Lawyer will complete the affidavit of service annexing the notification and a copy of the Solicitor General's advice.
15. The Case Lawyer will then make an appointment with the Common Law Duty Judge or, if the warrant is only for a tracking device and it is more convenient to do so, an eligible magistrate.
16. The Case Lawyer and deponent to the affidavit should attend the judge/magistrate. The following documents are placed before the judge or magistrate during the hearing of the application:
    (a) The affidavit deposing to the service of the section 51 notification;
    (b) The application;
    (c) The affidavit in support of the application and, if the judge indicates that he is prepared to grant the warrant sought;
    (d) The draft warrant.
17. If the application is granted the originals of the affidavits and application and a copy of the warrant (not the original warrant, which must be returned to the Commission) are then placed in a sealed envelope by the judge's associate/magistrate and retained on the courts file.

18. Upon return to the Commission the Case Lawyer will give the original warrant together with copies of all supporting documentation and the Authorisation Checklists to the Chief Investigator STU who will arrange for registration and retention of the documentation.
19. Upon notification that a warrant has been issued for the use of a surveillance device or devices a MOCCA (the Commission's computerised record system) case note should be prepared by the Case Officer indicating the time and date the warrant was issued, together with the expiry date and name of the issuing judge/magistrate. The Case Officer is to ensure that the Product Management Officer in STU is notified of the issue of the warrant. The Product Management Officer will create a task on 'Outlook' for 'submit section 44 report' and initiate an automatic expiry date reminder alert so as to enable the Case Lawyer sufficient time to prepare the section 44 Report.

Procedure 10A then goes on to set out the steps to be followed for urgent situations, extension or variation of a warrant, revocation of warrant, retrieval of devices, and section 44 reports. In addition the procedures for execution of the warrant, equipment, logs, disk handling care and storage, protection of surveillance device technologies and methods, transcription and notifying the subject of the surveillance are set out.

The procedure requires the Chief Investigator STU to:

(a) ensure the highest degree of security is afforded to the storing of all surveillance devices,
(b) be responsible for the installation, operational servicing and recovery of surveillance devices in accordance with warrants issued under the SD Act.
(c) liaise with any relevant outside agency regarding the installation, servicing and recovery of any device installed by that agency,
(d) purchase, modify, manufacture and provide surveillance device equipment and maintain a register of all such equipment in

possession of the Commission. The register is to include sufficient details of all surveillance devices to ensure accurate identification,

(e) ensure that relevant STU officers are trained in the use and installation of the surveillance devices and that sufficient STU members are available for immediate call,

(f) audit the register of surveillance devices equipment quarterly. Details of any losses, thefts, damage, destruction and device is outstanding at the expiration of a relevant warrant, must be brought to the attention of the Executive Director, ID.

Procedure 10B addresses the strict limitations imposed by section 40 of the SD Act on the use of "protected information", the record keeping requirements imposed by subsections 44, 46 and 47 of the SD Act and also the requirement to destroy any record or report obtained by use of a surveillance device under section 41(1)(b) of the SD Act.

6. CASE STUDIES

The Commission has published only one report into the cases studied in this audit. Accordingly, in respect of the remaining matters the description of the facts has been considerably abbreviated to prevent publication of any information which could adversely affect an ongoing investigation.

In each of the cases studied there has been complete compliance with the formal requirements of sections 17 (method and grounds of the application), 20 (contents of the warrant), 44 (Reports to eligible Judge or eligible Magistrate and Attorney General), and 51 (notification to Attorney General of particulars of the warrants sought) of the SD Act.

In addition, the requirements of ICAC's own Procedures 10A and 10B appear to have been fully followed. This includes the Authorisation Checklist being signed respectively by the Executive Director ID and the Executive Director Legal stating that a warrant is appropriate and that all documentation is approved.

WARRANT 1/2011

This application was made by an officer of the ICAC who was a law enforcement officer for the purposes of the SD Act seeking a warrant to authorise the use of one tracking device on a motor vehicle and three listening devices to be on or about the body of certain named persons.

The affidavit in support states that the application relates to an investigation by the ICAC of the relevant offence of obtaining a valuable thing by deception contrary to section 178 BA of the *Crimes Act 1900 NSW*.

The suspicion that the offence has been committed was based on the following facts:

A report had been received by the Commission of an allegation that two named persons who, by virtue of their employment with a company contracted to a Government Agency, had unlawfully accessed and downloaded strata plans

from the NSW Land and Property Management Authority (LPMA) strata plan database.

The named persons had ceased to be employed by the LPMA whereupon their authority to use and access the database ceased. Notwithstanding this it was noted that there had been an excessive downloading of strata plans from that database and the downloads were made using the user log-ons of the two former employees.

The LPMA reported that, between 1 May 2009 and 5 November 2009 under the log-on user names of the former employees, 74,771 of the LPMA's 80,000 strata plans had been unlawfully downloaded. The commercial value (being the amount that LPMA would normally charge to provide access to those strata plans) was $822,481. Enquiries revealed that the plans had been unlawfully downloaded to computers bearing certain IP addresses and those addresses were subscribed to by a private company and a university.

In light of the evidence it was believed that it was necessary for the purpose of an investigation to enable evidence to be obtained about the commission of the offence and the location of a named person on the following grounds:

- Commission officers had conducted physical surveillance of the named person who has been observed driving the subject vehicle;
- the Commission obtained telecommunications service warrants authorising the Commission to intercept communications made to or from the mobile phone of that and another person;
- a tracking device installed in the vehicle would facilitate the investigation by enabling the Commission to identify the location of any meetings between the named persons and others involved in the commission of the offence and the extent to which such meetings are conducted;
- in circumstances where such meetings take place in public the deployment of listening devices on or about the bodies of the Commission officers will enable them to record the conversations taking place at this meeting;

- although the privacy of persons would be affected only to the extent necessary to permit the effective investigation of the relevant offence in accordance with the provisions of the Act it was submitted that the gravity of the conduct constituting the offence was such it would justify the issue of the warrant. The use of the devices was expected to enable the Commission to gather evidence in an admissible form of the involvement of the named persons.

The request was that the warrant remain in force 90 days.

The warrant was issued by an eligible Judge of the Supreme Court for the period from 17:00 on 15 February 2011 until 17:00 on 15 May 2011.

The warrants were revoked pursuant to section 23 of the Act by an eligible Judge on 21 April 2011 following an application on the ground that the use of the devices authorised by the warrant were no longer necessary for the purpose of obtaining evidence to be obtained of the commission of the relevant offence or the identity of or location of the offender.

The report under section 44 of the Act to the Judge states that two of the devices were used pursuant to the warrant, namely a tracking device and a listening device. The activities of one of the named persons were recorded by the use of the tracking device and the private conversations of two of them were recorded or listened to by use of the listening device. The tracking device was used between 14:32 on 17 February 2011 and 14:00 on 6 April 2011. The listening device was used between 19:47 on 17 March and 21:56 on 17 March. The evidence obtained by use of the devices was of limited evidentiary value and was unlikely to be used in any future proceedings or investigations.

The Commission's report on its investigation into unauthorised copying of property information from the LPMA database published in November 2011 states that during the course of the investigation, the Commission:

- obtained documents from various sources by issuing 24 notices under section 22 of the ICAC Act (requiring production of documents);

- executed three search warrants to obtain information relevant to the investigation;
- undertook physical surveillance of persons suspected of being involved in corrupt conduct;
- interviewed and/or took statements from a number of persons;
- obtained three warrants under the relevant legislation to enable the interception of telecommunications;
- conducted nine compulsory examinations.

The Commission found that the subject engaged in corrupt conduct by providing other persons with her and another person's usernames and passwords in order to gain access to the LPMA database, knowing that she did not have authority to do so and that the access details would be used to gain access to the LPMA database to obtain information, free-of-charge, and by gaining access to the LPMA database by using the access details of another employee for the purpose of obtaining copies of strata plans for use in her work knowing that she did not have authority to do so and in order to avoid having to pay the prescribed fees to the LPMA.

WARRANT 2/2011

This application was for the use of two listening devices on the body of an investigator. The application related to an investigation by the ICAC of the relevant offence of corruptly soliciting a benefit contrary to section 249B(1) of the *Crimes Act 1900*.

Information had been received that an officer of a local government body had arranged for vehicles owned by the council to be sold at a price below value in return for a benefit of $500 to be shared between named council employees in return for them ensuring that a vehicle could be purchased from the council at the minimum reserve rate. In order to obtain evidence of the soliciting of a payment the use of two listening devices was sought.

The warrant was issued by an eligible Judge of the Supreme Court on 9 August 2011 for a period of 30 days commencing at 14:30 on 9 August 2011 and expiring at 14:30 on 7 September 2011.

Application was made for revocation of the warrant on the grounds that the use of the devices was no longer necessary.

The report under section 44 (1) of the SD Act revealed that the conversations of the named persons were listened to on six occasions on 11 August 2011. The information recorded by use of the listening devices did not contain information of any evidentiary value to the investigation.

WARRANT 3/2011

This application was for a warrant for the use of three listening devices on or about the bodies of certain named ICAC officers and related to the investigation by the ICAC of the relevant offence of corruptly receiving a reward contrary to section 249B(1) of the *Crimes Act 1900*.

Information had been received that a public official received benefits in return for the favourable exercise of his public functions.

The warrant was sought to authorise the use of the listening devices in respect of conversations between the persons alleged to be concerned in the commission of the offence. It was anticipated that the information sought to be obtained under the warrant would assist in the investigation by providing direct evidence from the named persons about the nature of their suspected involvement in the relevant offence.

The warrant was issued by a Justice of the Supreme Court who was an eligible Judge on 17 August 2011 for the period from 17:00 on 17 August 2011 until 17:00 on 15 November 2011.

An application was made for revocation of the warrant on the ground that the surveillance devices authorised by the warrant were no longer necessary for the purpose of enabling evidence to be obtained of the commission of the relevant

offence or the identity or location of the offender. The report under section 44 of the act states that one device authorised to be used by the warrant was used between 10:07 on 24 August 2011 and 10:48 on 24 August 2011. The evidence obtained by use of the device was of limited evidentiary value and is unlikely to be used in any future proceedings or investigations.

WARRANT 4/2011

The application was for a warrant for the use of one tracking device on or in a stated motor vehicle and related to the same investigation by the ICAC as is referred to in Warrant 3/2011.

The warrant was signed by a Magistrate who purported to sign as an eligible Magistrate. Subsequent inquiries alerted the Commission to the fact that the Magistrate who purported to issue the warrant was not an eligible Magistrate as defined by section 5 of the Surveillance Devices Act. Commission officers were unaware of this fact at the time they applied for the warrant on 18 August 2011. The tracking device was not installed in the named vehicle and was not used. A report of this was sent to the Solicitor General.

WARRANT 5/2011

Mr Roy Waldon, Solicitor to the Commission, advised that the authorisation checklist for this warrant was not filed with the other papers pertaining to the warrant. He has reminded the officers responsible for keeping warrant records of the need to ensure that each checklist is received from the investigator at the same time as the other warrant documentation. While he has not been able to locate the authorisation checklist, he is confident that one was prepared and signed as it is his practice not to approve the making of an application until he has seen a checklist signed by the Executive Director ID (or her delegate) and has himself signed that checklist. I accept this explanation.

This application related to the same investigation by the ICAC as is referred to in 3/2011. The application was for a warrant authorising the use of a tracking device on a named motor vehicle. The tracking device would facilitate the

ICAC's investigation into the relevant offence by enabling it to identify the location of any meetings conducted between the targeted persons. Where such meetings take place in public, the ICAC intended to deploy the listening devices previously authorised to record conversations taking place at that meeting.

The warrant was issued by an eligible Justice of the Supreme Court on 25 August 2011.

The report under section 44 of the Act states that the authorised surveillance device was not used pursuant to the warrant.

WARRANT 6/2011

This application was for a warrant for the use of one tracking device on or in a stated motor vehicle and related to the investigation by the ICAC of the relevant offence of corruptly receiving a reward contrary to section 249B (1) of the *Crimes Act 1900*.

Reliable information had been received that a public officer was providing illegal services in return for payment.

The tracking device was sought to provide the investigators with the means of identifying the movements of the target, with whom he meets and the places he frequents.

The warrant was issued by an eligible Justice of the Supreme Court on 21 December 2011 and was in force from 15:00 on 21 December 2011 to 15:00 on 19 March 2012.

The report, in accordance with section 44(1) of the SD Act dated 3 April 2012, delivered to the Solicitor General and the issuing Justice of the Supreme Court, reveals that the tracking device was used between 16:40 on 5 January 2012 and 12:40 on 19 March 2012 to identify the locations frequented by the target person. It also helped to identify persons associated with him, based on those places frequented. This led to further evidence being obtained.

7. CONCLUSION

During the twelve months period covered by this audit only five surveillance device warrants were validly sought and granted. (One was invalid because it was issued by a Magistrate who was not "eligible"). No applications were refused and no applications were made for a retrieval warrant. Only one of the warrants yielded material of evidentiary value.

It needs to be borne in mind that the decision to seek the issue of a warrant is made in the light of the information available at that stage. By the time of the execution of that warrant circumstances can, and often do, change. Consequently it is understandable that, on occasions, the changed circumstances at the time of execution may render the use of one or more of the devices unnecessary or not yield the hoped for result. This does not mean that the decision to apply for a warrant was unreasonable or improper.

The Commission has instituted and maintained a detailed and impressive system of controls designed to prevent an unauthorised or "rogue" application for a warrant under the SD Act in its Procedures 10A and 10B. It achieves this goal by requiring the participation of a number of its officers from different sections in the approval process.

Those officers include the Case Officer, the Case Lawyer, the Executive Director ID, the Chief Investigator of the Surveillance and Technical Unit (STU), the Case Officer's Chief Investigator, and the Executive Director Legal. The approvals of the Executive Directors of Investigations and Legal are required to be noted and actually appear on the Authorisation Checklist which accompanies the documentation.

In addition, the SD Act requires notification to the Attorney General seeking approval for the application for a warrant and the reply from the Solicitor General.

The procedures set out clear duties upon officers regarding the registration and retention of the documentation after the warrant has been authorised by the eligible Judge.

I have, pursuant to section 57B(2) of the ICAC Act, looked to see if there are grounds for reporting the existence of evidence of abuse of power, impropriety, or other forms of misconduct on the part of the Commission or officers of the Commission under section 57B(1)(b).

I have also looked to see if there were grounds for reporting the existence of evidence of maladministration including unreasonable invasions of privacy and action or inaction of a serious nature that is contrary to law, unreasonable, unjust, oppressive or improperly discriminatory or based wholly or partly on improper motives under section 57B(1)(c).

In addition I have assessed the effectiveness and appropriateness of the procedures of the Commission relating to the legality or propriety of its activities under section 57B(1)(d).

Examination of the applications for and executions of surveillance device warrants in each of the cases studied reveals the following:

- Surveillance device warrants were applied for and used as one of the tools authorised by the ICAC Act to enable the ICAC to carry out its functions;
- Each warrant was applied for only in circumstances where a belief was reasonably formed in the light of information available from other sources that the application was soundly based;
- In all cases it was appropriate to apply for and execute the surveillance device warrant in the light of the information then available;
- There was no evidence of abuse of power, impropriety, or other forms of misconduct on the part of the Commission or officers of the Commission;

- There was no evidence of maladministration, including unreasonable invasions of privacy, or of any action or inaction of a serious nature that was contrary to law, unreasonable, unjust, oppressive or improperly discriminatory or based wholly or partly on improper motives.

Harvey Cooper AM
Inspector
May 2012