Report of an audit of applications for and execution of listening device warrants by the Independent Commission Against Corruption

The Inspector of the Independent Commission Against Corruption

CONTENTS

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). One class of surveillance devices is listening devices. It is the ICAC's applications for and use of listening devices which is the subject of this audit.

A *listening device* means "any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear" (section 4 of the SD Act).

The use of listening devices to overhear and/or to record the conversations of persons without the knowledge of those persons is a serious intrusion into the right of privacy of those persons.

In addition, such use is a covert activity the presence of which is an unknown to the participants to those conversations. Consequently, those persons are not in a position to raise a complaint or protest.

On the other hand, there are circumstances in which the covert use of listening devices can provide evidence which can facilitate the 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 listening devices and the publication of the contents of conversations recorded by them goes on to authorise the ICAC covertly to use and record conversations in limited circumstances.

The purpose of this audit is to examine a sample of cases in which the ICAC has used listening devices to listen to and/or record conversations: --

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

This audit will cover the following: --

1. The Inspector's audit function
2. The ambit of the audit
3. An anomaly in the legislation and suggested amendments
4. The relevant provisions of the SD Act
5. ICAC's systems to control and regulate the application for and use of surveillance device warrants
6. Truth of the contents of affidavits
7. Case studies
8. Conclusions

1 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.

2 THE AMBIT OF THE AUDIT

By letter dated 21 May 2009 I wrote to the Commissioner in the following terms, omitting formal parts:

> Pursuant to section 57B of the *Independent Commission Against Corruption Act 1988* (the Act), I propose to audit and assess 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) limited to listening devices.
>
> The proposed audit and assessment will examine:
>
> 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 would, in the first instance, like to review 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 limited to Listening Devices during the period from 1 August 2008 to 31 January 2009, regardless of whether they were granted or refused by an eligible judge or magistrate.

Upon reviewing the materials identified above I may request further information from the Commission and/or its officers for the purpose of completing my audit and assessment. I welcome any comments you may have on the proposed ambit of this audit and assessment including any conditions you may require relating to the manner in which the information furnished to me will be dealt with.

The Commissioner replied by letter dated 29 May 2009 in the following terms, omitting formal parts: --

I refer to your letter dated 21 May 2009 advising that pursuant to section 57B of the ICAC Act you will conduct an audit and assessment of the effectiveness and appropriateness of the Commission's procedures in relation to the application for and execution of surveillance device warrants and retrieval warrants.

You have requested files and records relating to all applications for surveillance device warrants and retrieval warrants, limited to listening devices, for the period 1 August 2008 to 31 January 2009.

There have been no applications for retrieval warrants in this period.

Applications numbered SDW1 of 2008, SDW3 of 2008, SDW4 of 2008, SDW5 of 2008, SDW6 of 2008, and SDW7 of 2008 have been made in this period. The authorisation checklists, applications, affidavits in support, warrants, section 51(1) notices and section 44(1) reports for each of these applications

is enclosed. Application SDW2 of 2008 relates to tracking devices and therefore falls outside the scope of the information you request it.

No information relating to any of these applications is currently in the public domain.

The information sought by you and provided under cover of this letter comes within the definition of "protected information" as defined in section 39 of the Surveillance Devices Act 2007 (the SD Act). The SD Act places limitations on the use of communication of "protected information". Section 40 of the Act makes it an offence to communicate or publish "protected information".

Section 40(4) of the SD Act allows "protected information" to be published or communicated for the purpose of a "relevant proceeding". A "relevant proceeding" includes "an enquiry before the Inspector of the Independent Commission Against Corruption". The current audit and assessment would not appear to be "an enquiry before the Inspector of the Independent Commission Against Corruption".

Section 40(6) of the SD Act provides that a chief officer may consent to the communication of protected information if satisfied that it is necessary or desirable in the public interest for the protected information to be communicated to the person concerned and that the public interest in communicating the information out ways any intrusion of the privacy of the person to whom it relates or of any other person who may be affected by its communication. Section 40(7) provides that in deciding whether to give consent the chief officer must take into consideration the manner in which the protected information will be dealt with after it is communicated to the person concerned.

I have determined that it is in the public interest to provide the relevant “protected information” to you and enclose a copy of the signed consent.

3 ANOMALY IN THE LEGISLATION AND SUGGESTED AMENDMENTS

The Commissioner contends (in my view correctly) that the provisions of the SD Act to which he refers, *prima facie*, prohibit him from furnishing "protected information" to the Inspector for the purpose of an audit (as opposed to the purpose of a targeted inquiry). In the present case, applying sections 40(6) and 40(7), he has determined that it is in the public interest to provide the information and has done so.

This means that the Inspector's power to conduct an audit of the use of any surveillance device is dependant upon the willingness of the Commissioner to make a determination that it is in the public interest to provide the information.

This is contrary the provisions of section 57C of the ICAC Act which sets out the Inspector's powers, namely:

> The Inspector:
>
> (a) may investigate any aspect of the Commission's operations or any conduct of officers of the Commission, and
>
> (b) is entitled to full access to the records of the Commission and to take or have copies made of any of them, and
>
> (c) may require officers of the Commission to supply information or produce documents or other things about any matter, or any class or kind of matters, relating to the Commission's operations or any conduct of officers of the Commission, and
>
> (d) may require officers of the Commission to attend before the Inspector to answer questions or produce documents or other things relating to the Commission's operations or any conduct of officers of the Commission.

If the Inspector is to be able to exercise the duty of conducting audits in accordance with his powers, the SD Act should be amended by, for example adding a subsection (8) to section 40 to the effect that nothing in this section shall be deemed to limit the powers of the Inspector under section 57C of the ICAC Act.

The records of the ICAC relating to listening devices are inspected by the Ombudsman pursuant to section 48 of the SD Act. However, the Ombudsman merely checks the accuracy of the records – not the appropriateness of the application for and use of the device.

4 THE RELEVANT PROVISIONS OF THE SURVEILLANCE DEVICES ACT

A listening device means any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear (section 4 of the SD Act).

Section 7 prohibits the installation, use, causing to be used or maintain a listening device to overhear, record, monitor or listen to a private conversation to which the person is not a party, or to record a private conversation to which the person is a party. This, however, does not apply to the installation, use or maintenance of a listening device in accordance with a warrant.

Section 11 prohibits the communication or publication of private conversations or recordings of activities and section 12 prohibits the possession of a record of private conversation or activity.

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

> (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:-

(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.

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 number 10A entitled "Procedures For Obtaining and Executing Surveillance Device Warrants", the second is Procedure number 10B entitled "Procedures for Use and Recording Surveillance Devices Act Information". Both were approved on 10 April 2008 and the former was amended on 19 August 2008.

Procedure 10A contains general information regarding the definition of the 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 device is.

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 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 SDA, 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 SDA 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 SDA.

b. the affidavit deposing to the service of the section 51 notification.

10. The Case Lawyer will ensure that:

- all documentation meets the requirements of the SDA; and
- 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 SDU 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 an ICS 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 Act.

6 TRUTH OF THE CONTENTS OF AFFIDAVITS

A further aspect requiring consideration is whether the contents of the affidavits in support of the applications for warrants are true to the best of the applicant's knowledge and belief.

It is neither possible nor practicable to cross-examine every deponent upon every affidavit. However, examination of the facts set out in the affidavits in support reveals that the belief was held by reason of information obtained from individuals, lawfully obtained telephone intercepts or surveillance devices or from the results of previous searches. The results of these prior activities are registered and recorded within the premises of the ICAC and any discrepancy between the contents of the affidavit and those records would be readily apparent to the senior officers whose approval is required. Furthermore, an examination of each application shows an internal consistency of information together with internal support for the conclusions derived and raises a high degree of probability that the contents of those affidavits were true and correct.

7 CASE STUDIES

It is noted that the Commissioner's letter of 29 May 2009 (see above) states that no information relating to any of these cases is currently in the public domain. Consequently, to prevent publication of any prohibited information the description of the facts of each case has been considerably abbreviated.

In each case there has been complete compliance with the formal requirements of sections 17, 20, 44 and 51 of the SD Act.

In addition the requirements of ICAC's own Procedures 10A and 10B appear to have been fully followed including the Authorisation Checklist.

File Number 1/2008

This surveillance device warrant was issued on 18 September 2008 authorising the use of seven listening devices at the premises of a government agency in respect of conversations of named persons. The warrant was in force from 6 pm on 18 September 2008 until 6 pm on 15 October 2008.

The section 44(1) report was to be furnished within 14 days of the expiration of the warrant.

The affidavit in support of the application sets out in considerable detail the matters required under the SD Act including the basis for believing that the use of the surveillance devices on the subject premises was necessary for the purpose of investigation into the offence of corruptly receiving a benefit contrary to section 249B(1) of the *Crimes Act* 1900 (The Crimes Act) and aiding and abetting the commission of that offence contrary to section 249F(1) of the same Act.

The Solicitor General was notified of the intention to apply for the warrant and advised that the Attorney General did not wish to be heard on the matter. The authorisation checklist was duly completed.

The report pursuant to section 44(1) of the SD Act reveals that the surveillance devices authorised by the warrant were used pursuant to the warrant and that they were listening devices. The private conversations of the named persons were recorded or listened to by use of the devices. On one date all persons named were present when the listening devices recorded the conversations. The report goes on to say that due to the number of persons in the proximity of the listening devices and acoustics of the room it was difficult to distinguish the entirety of the recorded conversation and as such the recordings will not be used in evidence in any Commission or criminal proceedings. On a further day within the period of the warrant a person named was present when a recording was made. The recording did not contain any information relevant to the involvement in the matters under investigation.

Recordings of persons other than those named in the warrant were destroyed without being reviewed.

File Number 3/2008

This surveillance device warrant was issued on 26 September 2008 authorising the use of two listening devices at the premises of a Government agency in respect of conversations of certain named persons. The period of the warrant was from 8 pm on 26 September 2008 until 8 pm on 23 October 2008.

The alleged offences in respect of which the warrant was issued are corruptly receiving a benefit contrary to section 249B(1) of the Crimes Act and aiding and abetting the commission of that offence contrary to section 249F(1) of the same Act.

The affidavit in support of the application shows that the investigation followed on from the investigation referred to in the preceding file. It also sets out the reasons for the belief that the use of listening devices was necessary for the purpose of an investigation into the offence to enable evidence to be obtained of the commission of that offence and also the reasons for the belief that there was no alternative means of obtaining evidence of similar reliability.

The Authorisation Checklist shows that information giving rise to the need to seek authorisation to make an application for the warrant became available late on Friday, 26 September 2008 after the Executive Director, ID had left the Commission's premises for the weekend. The relevant information was communicated to him by telephone and e-mail and later that night the Executive Director ID gave approval for the activity to proceed.

The report in accordance with section 44(1) of the SD Act states that the listening device was used to record private conversations of the named persons which occurred on 28 September 2008. The device recorded the private conversations of those persons during which information was obtained relevant to their involvement in the matters then under investigation by the Commission. The information obtained was used to inform questions asked of a named person when that person attended and gave evidence in Commission proceedings. It was not anticipated that the recording of the conversation would be used in any future criminal proceedings.

File number 4/2008

This surveillance device warrant was issued on 17 November 2008 and authorised the use of five listening devices in respect of conversations, activities and geographical location of three named persons. It was for the period from 2.30 pm on 17 November 2008 until 2.30 pm on 16 December 2008.

The affidavit in support reveals facts giving rise to a reasonable belief that the named persons had committed the offence of common law conspiracy to cheat and defraud. From information available it was reasonably believed that they would be meeting at premises in a named regional town. It was considered likely that a conversation regarding the scheme to cheat and defraud would occur during a planned meeting. It also points out that while other methods could assist the investigation to a limited extent, they would not produce evidence of similar reliability to that which would be obtained by means of listening devices.

The report in accordance with section 44(1) of the SD Act says that the devices authorised by the warrant were used and that private conversations of the three named persons and an unknown person were recorded or listen to by use of the devices. The material recorded, however, did not contain information of any evidentiary value to the investigation by the Commission.

File Number 5/2008

This warrant was issued on 17 November 2008 and authorised the use of the listening devices on or about the body of covert ICAC identities. It authorised the use of the devices in respect of conversations and activities of three named persons in respect of the investigation by the commission of a serious fraud constituted by the common law offence of conspiracy to cheat and defraud.

The period of the warrant was from 2.30 pm on 17 November 2008 until 2.30 pm on 16 December 2008.

The alleged illegal activities were the same as those set out in file number 4/2008.

The report in accordance with section 44(1) of the SD Act reveals that the private conversations of the three named persons and another unknown persons were recorded or listen to by use of the listening devices but the material recorded did not contain information of any evidentiary value to the investigation by the Commission.

File Number 6/2008

This surveillance device warrant was issued on 10 December 2008 and authorised the use of a listening device on or about the body of a named person on certain premises. The warrant authorises the use of the device in respect of conversations of three named persons and any other persons as yet unidentified who may be involved in the offence of corruptly receiving a benefit contrary to section 249B(1) of the Crimes Act.

The period of the warrant was from 12.00 pm on 10 December 2008 until 12.00 pm on 22 December 2008.

The affidavit in support of the application sets out facts relating to the alleged offence and the involvement of the named persons therein. One listening device was proposed to be used on the premises and two on or about the body of a named person. It was anticipated that a meeting would occur at 3.00 pm on 10 December 2008 at which a corrupt payment would be made and that the use of the listening device would furnish reliable evidence of the Commission of the offence by providing direct evidence of conversations taking place at the time of the offence.

The report in accordance with section 44(1) of the SD Act states that the surveillance devices authorised by the warrant were not used.

File Number 7/2008

On 15 December 2008 approval was sought to make application for a further two listening devices on application 7/2008. In total the application would be seeking four devices with the remaining 2 to be on or about the body of a law enforcement participant for the purpose of a controlled operation as per a previous approval. Approval was given on 16 December 2008.

The surveillance device warrant was issued on 16 December 2008 authorising the use of listening devices on or about the bodies of 11 named persons in respect of conversations of 10 named persons and other persons as not yet identified who may be involved in the offences of using false or misleading documents by an agent with intent to defraud the agent's principal contrary to section 249C(1) of the Crimes Act and aiding and abetting the commission of an offence of using false or misleading documents by an agent with intent to defraud the agent's principal contrary to section 249C(1) of the Crimes Act and being an offence contrary to section 249F of the Crimes Act.

The affidavit in support sets out facts alleging that a Government agency was suspected of fraudulently issuing certain certificates to applicants in exchange for corrupt payments from those applicants.

As a result of all of the information received from a number of sources it was believed that the use of four surveillance devices were necessary for the purpose of investigating the relevant offences and to enable evidence to be obtained of the commission thereof.

The report in accordance with section 44(1) of the SD Act states that the activities of 6 named persons were recorded or listened to by the use of the devices on 17,18 and 19 December 2008 and 7, 9, 12, 13, 14, 21, 22, 27, and 28 January 2009.

The evidence was used to progress the Commission's investigation and is likely to be used in future proceedings conducted by the Commission and any criminal proceedings recommended by the Commission for prosecution by the Director of Public Prosecutions.

The listening devices were used to record conversations between two named persons during an authorised controlled operation. The recorded conversations indicate that one person provided another with falsely issued certificates in return for payment of money.

The devices also were used to record conversations between two named persons during an authorised controlled operation during which one sought the assistance of the other in obtaining a certificate and indicated that one agreed to assist the other only if he could provide certain paperwork but did not provide evidence of one named person having engaged in corrupt conduct or criminal activity. The evidence obtained by use of the devices was used to progress the Commission's investigations and it is unlikely to be used in any future proceedings or investigations.

The listening devices were also used to record conversations between two named persons during an authorised controlled operation during which one sought the assistance of the other in obtaining certain certificates. The recorded conversations indicate that the assistance would be provided only upon provision of verifiable paperwork but did not provide evidence of one having engaged in corrupt conduct or criminal activity. The evidence obtained by use of the devices was used to progress the Commission's investigation and is unlikely to be used in any future proceedings or investigation.

The devices were also used to record private conversations between two named persons. It provided no evidence of one having engaged in corrupt or criminal activity but did confirm that they had prior association. The evidence

obtained by use of the devices was used to progress the Commission's investigation and is unlikely to be used in any future proceedings or investigations.

8 CONCLUSION

The Commission has instituted and maintained a detailed and impressive system of controls designed to prevent the 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 large 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, the Executive Director Legal and the Product Management Officer in the STU. 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 upon 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 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 attempted to assess the effectiveness and appropriateness of the procedures of the Commission relating to the legality or propriety of its activities (section 57B(1)(d)).

Examination of the application for and execution of surveillance search warrants in each of the cases studied reveals the following:

- Surveillance Device warrants (limited to listening devices) 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.

- In all but those cases where execution was not undertaken or where execution revealed no evidential material, the issue and execution of the surveillance device warrants were effective in locating material which contributed to the investigations of the Commission;

- 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