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

April 2011

by
The Inspector of the
Independent Commission Against Corruption

Table of 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).

During the course of conducting previous audits it became apparent that warrants for the use of more than one class of surveillance device would be sought in the one application.

Accordingly, 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 period from 1 January to 30 June 2010.

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 that such use is limited to those circumstances where it is lawful and appropriate for the conduct of its statutory functions.

- 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) Case studies
7) 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 14 December 2010 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).
>
> 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 Data, Optical and Tracking Surveillance Devices during the period from 1 February 2009 to 30 June 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 Commission replied by letter dated 12 January 2011 advising that three 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.

The letter continues:

> The documentation 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 outweighs 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.
>
> The Commissioner has determined that it is in the public interest to provide the relevant “protected information” to you and I enclose a copy of the Commissioner’s 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, therefore, done so.

This means that the Inspector's power to conduct an audit of the use of any surveillance device is dependent 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.

As pointed out in my last Annual Report, my requests for such an amendment have remained unsatisfied.

The records of the ICAC relating to listening devices are inspected by the NSW Ombudsman pursuant to section 48 of the SD Act. However, the NSW 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

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:

(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 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 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

A Report into one of the cases studied has been published. In respect of the remaining matters the description of the facts of each case 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, 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.

Warrant 1/2010

This warrant was issued on 29 March 2010 authorising the use of two tracking devices and three listening devices in connection with the investigation of the offence of corruptly receiving benefits contrary to section 249B(1) of the *Crimes Act 1900*.

One of the tracking devices was to be attached to a vehicle used by Hedley Peter Higgs (referred to in the warrant as Peter Hedley Higgs) and the second to a vehicle used by Thomas David Turner. The three listening devices were to be on or about the bodies of Commission officers.

The tracking devices were to enable Commission surveillance officers to locate the position of the targets and the listening devices were to enable those officers to place themselves in the vicinity of the targets and record their conversation.

The warrants expired at 3:30 PM on 26 June 2010.

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 signed by the Executive Director, Investigation

Division and the Executive Director, Legal in accordance with the ICAC's procedures.

The report pursuant to section 44(1) of the SD Act states that two surveillance devices, being the two tracking devices, authorised by the warrant were used pursuant to the warrant and that that the activities of the targets were recorded and listened to by the use of these listening devices.

The report further states that the material recorded did not contain evidence of evidentiary value and therefore would not be used in any Commission or criminal proceedings.

In its report on the *Investigation Into The Acceptance of Corrupt Benefits by a City Of A Canada Bay Council Employee* published in December 2010 the Commission sets out details of the contradictory nature of the evidence provided by the named persons and the acts undertaken by them to conceal and fabricate evidence.

The report states that during the course of the investigation the named persons clearly embarked on course of action to mislead the Commission.

Whilst the use of these five surveillance device warrants did not yield any probative evidence the warrant was a legitimate part of the Commission's strategy of using various investigative tools to ensure that it was not misled. These tools included compulsory examinations, issuing notices under sections 21 and 22 of the ICAC Act and use of covert surveillance.

Following upon a public inquiry the Commission made findings that Mr Hedley Peter Higgs, an employee of the City of Canada Bay Council (CCBC) and Mr Thomas David Turner, the owner of an excavation and concreting company and a contractor to CCBC, had engaged in corrupt conduct. The Commission recommended that the advice of the Director of Public Prosecutions (DPP) should be obtained in respect of the prosecution of Mr Higgs for offences of:

- receiving corrupt rewards from Mr Turner and Mr Hraichie, contrary to section 249B(1) of the *Crimes Act 1900.*
- giving false and misleading evidence, contrary to section 87(1) of the ICAC Act.
- fabricating a document with the intent to mislead the Commission, contrary to section 88(3) of the ICAC Act.

The Commission also recommended that the advice of the DPP should be obtained with respect to the prosecution of Mr Turner for offences of:

- giving a corrupt benefit to Mr Higgs, contrary to section 249B(2) of the *Crimes Act 1900.*
- giving false and misleading evidence, contrary to section 87(1) of the ICAC Act.
- fabricating a document with the intent to mislead the Commission, contrary to section 88(3) of the ICAC Act.

Warrant 2/2010

This surveillance device warrant was issued on 8 June 2010 authorising the use of three listening devices on or about the bodies of named Commission officers to record conversations between targets of the investigation alleged to have, as an agent, corruptly received benefits contrary to section 249B(1) of the *Crimes Act 1900* (the Crimes Act). The warrant was in force from 4.15 pm on 8 June 2010 until 4.15 pm on 5 September 2010.

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, which was made on an urgent basis, sets out in considerable detail the matters required under the SD Act. It included the basis for believing that the use of the surveillance devices was necessary to

investigate the offence of corruptly receiving a benefit contrary to section 249B(1) of the Crimes 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 signed by the Executive Director, Investigation Division and the Executive Director, Legal in accordance with the ICAC's procedures.

The report pursuant to section 44(1) of the SD Act reveals that the surveillance devices authorised by the warrant were not used pursuant to the warrant.

At the time of writing, the investigation in respect of which the search warrant was obtained is still current. In order not to prejudice the investigation I am unable to disclose further details. I have, however, formed the view based on my inspection of the relevant warrant application and report documents that, given the information then available to the Commission, the application for the warrants was reasonable and appropriate for the furtherance of its investigations.

Warrant 3/2010

This warrant was issued on 15 June 2010 authorising the use of two listening devices to be used to record conversations of named persons said to have knowledge of the offence of corruptly receiving benefits contrary to section 249B (1) of the Crimes Act. It relates to the same investigation as a warrant 2 of 2010.

The warrant was in force from 10 a.m. on 15 June 2010 until 10 a.m. on 12 September 2010.

A meeting was due to take place and the warrant was required to permit the use of the listening device lawfully to record the conversation at that meeting which was reasonably expected to cover matters, the subject of the investigation.

Notification was duly served on the Attorney General and the appropriate response was received.

The report under section 44 of the SD Act states that the listening device was used between 15:05 and 16:52 on 16 June 2010 but that the material recorded contained no information of material value to the investigation and would not be used in relation to any public enquiry or for the prosecution of charges arising from the investigation.

Nonetheless, at the time of applying for the warrant it was reasonable to believe that the conversation to be recorded would yield probative evidence relevant to the investigation. I am, therefore, satisfied that the application for the warrant was reasonable and appropriate for the furtherance of ICAC's investigation.

7 CONCLUSION

During the six months period covered by this Audit only three surveillance device warrants were sought and granted - no applications were refused and no applications were made for a retrieval warrant.

None of the material recorded by listening devices so authorised 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 occasion, the 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, 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 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, examined 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 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

April 2011