Report of the Victorian Inspectorate to the Parliament of Victoria Pursuant to the *Surveillance Devices Act 1999*

Report No. 1 of 2012 - 2013

5 March 2013

Table of Contents

List of Abbreviations

CCP	Chief Commissioner of Police
DPI	Department of Primary Industries
DSE	Department of Sustainability and Environment
ESD	Ethical Standards Department (Victoria Police)
OPI	Office of Police Integrity
PI	Protected Information
PIR	Protected Information Register(s)
SD Act	*Surveillance Devices Act 1999* (Vic)
SIM	Special Investigations Monitor
SPU	Special Projects Unit (Victoria Police Intelligence and Covert Operations)
VI	Victorian Inspectorate

INTRODUCTION

The *Surveillance Devices Act 1999* (Vic) (the SD Act) regulates the use of surveillance devices in the State of Victoria. The SD Act makes provision for warrants and emergency authorisations permitting the installation, use, maintenance and retrieval of surveillance devices by four State law enforcement agencies.[1] Use of surveillance devices in relation to private activity and private conversations is otherwise generally unlawful in Victoria.[2]

The SD Act imposes a regime of strict controls relating to the use of surveillance devices, including a requirement for agencies to make and keep records and documents and to destroy certain material when it is not likely to be further required for an authorised purpose. It also provides for the inspection of agency records and documents by an independent officer who is responsible directly to the Victorian Parliament. Between 1 July 2006 and 9 February 2012 the inspection function was the responsibility of the Special Investigations Monitor (SIM), a statutory officer whose responsibilities included inspecting agency records, assessing statutory compliance with the SD Act and reporting to the Parliament.

Transfer of responsibility to the Victorian Inspectorate

Following the introduction by the Government of a suite of legislative changes to Victoria's integrity system, the office of the SIM was abolished on 10 February 2013. The functions previously performed by the SIM were transferred, with minor modifications, to a new body, the Victorian Inspectorate (VI). The VI has taken possession of all information, documents and records previously held by the SIM, and has taken over the SIM's work in progress.

Under section 30Q of the SD Act, the SIM was required to make six-monthly reports to Parliament. When the new legislation came into force on 10 February 2013, the report of the SIM in respect of the period from 1 July 2012 to 31 December 2012 had not been completed. Under the transitional provisions of the new legislation[3] it

[1] The SD Act also permits the Australian Crime Commission (ACC) to use the provisions of the Act. Inspection of ACC records and documents is conducted by the Commonwealth Ombudsman pursuant to s. 55(2) of the *Surveillance Devices Act 2004* (Cth).
[2] The SD Act provides for certain exceptions at ss. 5, 6(2), 7(2), 8(2), 9(2), 9B(2)(b) and (c), 9C(2).
[3] SD Act s. 43(11).

became the responsibility of the VI to complete that report and present it to Parliament.

This report is therefore submitted to the Parliament of Victoria and to the Minister responsible for the SD Act (the Attorney-General) in accordance with s. 30Q of that Act. It details the results of inspections conducted of agency records between 1 July 2012 and 31 December 2012 together with any other statutory compliance matters of note.

KEY PROVISIONS OF THE SD ACT

Purposes of the SD Act

The purposes of the SD Act include -

- the regulation of the installation, use, maintenance and retrieval of surveillance devices
- the establishment of procedures for law enforcement officers to obtain warrants or emergency authorisations for the installation, use, maintenance and retrieval of surveillance devices
- the imposition of requirements for the secure storage and destruction of records and for the making of reports to judges, magistrates and the Parliament in connection with surveillance device operations
- the recognition (subject to the *Surveillance Devices Regulations 2006*) of warrants and emergency authorisations issued in another jurisdiction authorising the installation and use of surveillance devices.[4]

[4] Section 1.

Agencies permitted to use surveillance devices

Four State law enforcement agencies are permitted to apply for a surveillance device warrant:

- Victoria Police
- Office of Police Integrity (OPI)
- Department of Primary Industries (DPI)
- Department of Sustainability and Environment (DSE).

Types of surveillance device

The SD Act permits the use of the following surveillance devices:

- data surveillance devices
- listening devices
- optical devices
- tracking devices

Subject to obtaining appropriate authorisation, the use of devices for multiple functions is permitted.

Warrants and emergency authorisations

SURVEILLANCE DEVICE WARRANTS

Sub-section 15(3) of the SD Act provides that a surveillance device warrant application must be made to a judge of the Supreme Court of Victoria or, in the case of an application for one or more tracking devices only, to a magistrate. The application must be made by an officer of one of the law enforcement agencies referred to above. There is also provision for a 'remote application' to be made by

telephone, fax, email or other means of communication in circumstances where it is impractical for an application to be made in person.[5]

EMERGENCY AUTHORISATIONS

The SD Act makes provision for an emergency authorisation to be granted by a 'senior officer'[6] for use of a surveillance device where there is an imminent threat of serious violence to a person or of substantial damage to property[7] or where the intended use of a device relates to a serious drug offence.[8] These emergency provisions may be exercised only in specified circumstances, where the seriousness and urgency of the situation justifies the use of a surveillance device but it is not practicable to apply for a warrant. Emergency authorisation may be given if the senior officer is satisfied that there are reasonable grounds for the applicant's suspicion or belief founding the application. During the period covered by this report, an application for an emergency authorisation could be made only by an officer of the Victoria Police or the OPI.[9]

When an emergency authorisation is granted, a senior officer (or another person acting on his or her behalf) must apply within two business days to a Supreme Court judge for approval of the exercise of powers under that authorisation.[10]

RETRIEVAL WARRANTS

Provision is made under the SD Act for the issue of a retrieval warrant to authorise the recovery of a surveillance device where the device was lawfully installed on premises or in or on an object. As a surveillance device warrant authorises installation and retrieval within the period of the warrant, a retrieval warrant is usually only necessary where the device is not retrieved within the authorised period and retrieval might otherwise constitute a trespass or other offence. The procedure for the issue of retrieval warrants is governed by ss. 20C to 20G of the SD Act.

---

[5] Section 16.
[6] Defined in s. 3.
[7] Section 26.
[8] Section 27.
[9] Section 25 specifically excludes the DPI and the DSE. Under the new legislation in force as from 10 February 2013, an officer of the Independent Broad-Based Anti-Corruption Commission may also apply for an emergency authorisation.
[10] Section 28.

REVOCATION

A surveillance device or retrieval warrant may be revoked by a Supreme Court judge if it was issued by a judge, or a by magistrate if it was issued by a magistrate.[11]

The SD Act also requires the chief officer of a law enforcement agency to revoke a surveillance device warrant when he or she is satisfied that the need for using the authorised device(s) to obtain evidence of the commission of an offence, or to establish the identity or location of an offender, no longer exists.[12] There is a similar provision requiring revocation of a retrieval warrant if the grounds for the application cease to exist during the period of the warrant.[13]

EXERCISE OF POWERS

Certain powers[14] under the SD Act may be exercised by either senior officers[15] of the agency concerned or authorised police officers.[16]

In addition, in respect of Victoria Police, the Chief Commissioner of Police (CCP) has a general power pursuant to s. 6A of the *Police Regulation Act 1958* to delegate (subject to stated exceptions) the exercise of any power, discretion, function, authority or duty of the CCP.

The role of the Special Investigations Monitor

During the period covered by this report, the SIM was the entity responsible for inspecting agency records and reporting the level of statutory compliance achieved to the Parliament.

More particularly, the SIM was required by s. 30P of the SD Act to inspect the records of Victorian law enforcement agencies using surveillance devices under a warrant or emergency authorisation in order to determine the level of statutory compliance by the agency and its law enforcement officers.

---

[11] Sections 20A(1) and 20H(1).
[12] Sections 20A(2) and 20B(2).
[13] Section 20H(3).
[14] For example, see ss. 15(2) and 20C(2).
[15] Defined in s. 3.
[16] Defined in s. 3.

The SD Act, as in force until 9 February 2013, required inspections by the SIM to be carried out 'from time to time'.[17] The SIM was required to report to the Parliament on the results of each inspection as soon as practicable after 1 January and 1 July of each year.[18] The SIM was also required to provide a copy of each report to the Minister (Attorney-General).

As previously noted, this report was not completed until after the SIM had ceased to exist and the functions of the SIM had been transferred to the VI, including the function of completing this report.

The inspection powers of the SIM under the SD Act

During the period covered by this report, the SIM, pursuant to s. 30P of the SD Act -

- having first notified the chief officer of the relevant law enforcement agency, was entitled at any reasonable time to enter the premises occupied by the agency
- was entitled to have free access at all reasonable times to the relevant records of the agency
- was entitled to require a member of staff of the agency to provide such information as the SIM considered relevant to the inspection.

INSPECTION OF STATE AGENCIES

Introduction

This report addresses the results of inspections undertaken by the SIM during the period 1 July 2012 to 31 December 2012.

Assessing compliance

The SIM's role included assessment of and reporting on agency compliance with the SD Act. In practical terms the inspection of records focused on specific statutory

[17] Section 30P(1).
[18] Section 30Q.

obligations with which agencies must comply. These relate to the manner of obtaining warrants, the use of using surveillance devices, the keeping of required records and compliance with the restrictions imposed under Part 5 of the SD Act in relation to the use, communication, publication and reporting of information.

Inspection of warrant files and other records

For the purposes of this report, the SIM continued to inspect warrant files on the basis detailed in Report 1 for 2009-2010.[19] Accordingly, a file was inspected only after all statutory reporting requirements referrable to that warrant had been completed. This method negates the need for inspection officers to return to warrant files to address matters not finalised at the time of first inspection. To date, sampling has not been necessary.

It is intended that Victoria Police surveillance device warrant files will continue to be inspected three times in each financial year. Related records made or held by investigators will be inspected bi-annually (once in each half of the financial year). The other three agencies, having relatively fewer warrants, will be inspected bi-annually,[20] at which time both warrant files and other records will be inspected concurrently.

Understanding 'Protected Information'

Before reporting inspection results, it is useful to note that the SD Act limits the use, communication and publication of 'protected information' (PI), which is defined as including –

- information obtained through use of a surveillance device authorised by a warrant or an emergency authorisation;
- information about an application for a warrant (including a retrieval warrant) or emergency authorisation; and

[19] Report of the Special Investigations Monitor pursuant to the *Surveillance Devices Act 1999* – Report No. 1 of 2009-2010.
[20] Except in circumstances where there are no records to inspect. Having not applied for a warrant under the SD Act, DSE did not require inspection in the period under report.

- information about an application for approval of use of emergency powers.[21]

The SD Act also requires that records or reports obtained by use of a surveillance device be kept secure and inaccessible to unauthorised persons.[22] Accordingly, an agency must keep all PI secure, including not only the reports and records obtained by the use of a surveillance device, but also associated information and documents connected to the issue of the warrant or emergency authorisation.

For the purpose of this report the term 'PI' is used when referring to information obtained from the use of a surveillance device, although as noted above the statutory definition is much wider.

[21] Section 30D.
[22] Section 30H.

DEPARTMENT OF SUSTAINABILITY AND ENVIRONMENT

The DSE did not obtain nor seek any warrants under the SD Act in the period under report.

The DSE has not obtained nor sought a warrant in the period since 1 July 2006.[23]

[23] This being the date the SIM assumed responsibility for agency inspections.

DEPARTMENT OF PRIMARY INDUSTRIES

The DPI obtained two new warrants in the period under report. These were obtained for the use of tracking devices only. Both warrants were executed and, pursuant to s. 30K of the SD Act, reports were made to the magistrate who issued the warrants.

Two compliance matters were identified by the inspecting officers with respect to the s. 30K Reports. The first matter was that each report incorrectly stated one of the names of the persons involved in the execution of the warrants.[24] This was a significant error and although it is considered that it was accidental, the SIM was of the view, and the VI agrees, that particular care should be taken in the future. The second matter was that each report inaccurately stated the period during which the devices were used.[25] In relation to the latter matter, the use of the device was in each case within the period the relevant warrant was in force, but the reporting of the dates of that use was inaccurate.

A further issue identified by the inspecting officers related to the warrants themselves. Neither warrant specified a time within which a report to the issuing judge or magistrate was required to be made under s. 30K of the SD Act. The specification of such a time is a requirement of s. 18(1)(b)(xi) of the SD Act.

The omission was not detected by the magistrate who issued the warrants but was subsequently identified by the agency. The agency then applied to the issuing magistrate for a report time to be set for each warrant, and this occurred. The agency subsequently reported within that time.

The SIM considered that the failure to include the report time in the two warrants was an oversight, and that the action taken by the agency to correct the oversight was entirely appropriate. The VI agrees with that assessment.

Agency staff advised the SIM's inspecting officers that as a result of the omission of a reporting time in each warrant, the agency would review the template from which warrants are prepared and ensure it includes provision to state the time within which a report must be made.

[24] Section 30K(2)(b)(i).
[25] Section 30K(2)(b)(iii).

In relation to that template, the SIM considered, and the VI agrees, that a good precedent is to be found in the *Supreme Court (Criminal Procedure) Rules 2008* (Vic). While the SD Act does not require that a warrant be in a prescribed form, those Rules contain an optional surveillance device warrant pro-forma, which includes, inter alia, a statement of the time within which a report pursuant to s. 30K must be made to the issuing judge.[26] These Rules are not directly applicable in the circumstances, as they apply only in relation to applications for surveillance device warrants that are made to a judge of the Supreme Court, and each of the warrants in question was issued by a magistrate. However the SIM considered, and the VI agrees, that it would be good practice for agencies to adopt the Supreme Court Form, with amendments where required, for all surveillance device warrants obtained under the SD Act, including those issued by a magistrate.

Except in relation to the matters referred to above, the agency was compliant with the requirements of the SD Act. The result of the DPI using surveillance devices irregularly is that agency staff are not likely to acquire specialist knowledge of the SD Act. Furthermore, the SIM understood, and the VI agrees, that agency staff who are required to consider the SD Act provisions at an operational level are not legally trained. Accordingly, it is not greatly surprising that compliance issues may arise. In these circumstances, establishing legal oversight within the DPI of the administration of surveillance device warrants may assist in achieving full statutory compliance.

[26] *Supreme Court (Criminal Procedure) Rules 2008* (Vic) Order 7.05.

OFFICE OF POLICE INTEGRITY

Three surveillance device warrant files were inspected in the period under report. All three warrants had been executed.

Inspecting officers identified two compliance issues in respect of details entered in the Register required to be kept in accordance with s. 30O of the SD Act. The first issue was that the date of issue of each warrant was incorrectly entered in the Register.[27] The second issue was that there were errors in the detail entered regarding variations or extensions of the warrants.[28] The inspecting officers informed the agency of these errors, which were subsequently corrected by OPI staff.

Other compliance requirements under the SD Act were fully met in respect of the three warrants.

[27] Section 30O(2)(a).
[28] Section 30O(2)(f).

VICTORIA POLICE

Introduction

Victoria Police has two units administering surveillance device warrants. The Special Projects Unit (SPU) manages warrants for the Crime Department, Regional Criminal Investigation and Response units and other operational units. The Ethical Standards Department (ESD) manages warrants obtained in respect of ESD investigations. ESD also occasionally assists SPU in managing warrants for other units.

Although warrant administration is centralised at SPU or ESD, the storage, use and destruction of information obtained from use of surveillance devices is the responsibility of investigators and Regional command. Investigators keep a Protected Information Register (PIR) for each surveillance device warrant, in which certain records required by the SD Act are kept.

Inspection Results

Overall, Victoria Police achieved a high level of compliance with the statutory requirements of the SD Act. Notwithstanding the good overall result, some problems were identified in relation to records kept by investigators and the content of reports made pursuant to s. 30K of the SD Act.

Warrant files administered by SPU and ESD were inspected in August and December 2012. In total, 101 surveillance device warrant files, two retrieval warrant files and two emergency authorisation files were inspected in the period under report. These comprised the warrants and emergency authorisations that ceased to be in force in the period between 1 January and 31 August 2012.

In addition, a total of 59 PIRs held by investigators were inspected in October to November 2012.

Forty two of the 59 inspected PIRs were being inspected for the first time, or had been issued at the time of the previous inspection and were expected to contain entries made after that inspection.

Seventeen of the 59 inspected PIRs were being re-inspected for the purpose of assessing whether or not register errors (omissions or mistakes) detected at the previous inspection had been rectified.

Three of the 17 PIRs re-inspected also contained 'new' entries that had been made after the inspection at which errors had previously been identified. Accordingly, those three PIRs were inspected not only to assess whether previously identified errors had been rectified, but also to assess compliance of the new entries with paras. 30N(c), (d) and (e) of the SD Act.

It should be noted that the inspection of PIRs was undertaken between the two inspections of warrant files. Accordingly, the number of PIRs being reported on is significantly fewer than the total number of warrant and emergency authorisation files under report.

PIRs were inspected at Crime Department squads and other investigation units across Melbourne and regional Victoria.

Investigator register records

A large number of records are made in PIRs by members of Victoria Police in compliance with paras. 30N(c), (d) and (e) of the SD Act. These provisions require a record to be kept of each use of PI, each communication of PI to a person other than a member of Victoria Police, and each occasion in a proceeding when PI is given in evidence.

Given the large number of entries made in PIRs across the agency it is inevitable some errors (whether omissions or mistakes) will occur. The issue for the SIM when considering compliance is the frequency of such errors. Accurate PIR records are essential not only to ensure compliance with paras. 30N(c), (d) and (e), but also because omissions or errors in these records may lead to consequential omission or inaccuracy in reports made under s. 30K to the judge or magistrate who issued a warrant.

Registers containing 'new' entries

Table 1 below summarises the results of the inspection of the 45 PIRs which contained 'new' entries.[29] The Table divides errors into the following categories:

- 'Use' errors, which are errors in recording the details of use of information obtained by the use of a surveillance device as required by s. 30N(c) of the SD Act

- 'Communication' errors, which are errors in recording the details of each communication to a person (other than a law enforcement officer of the agency) of information obtained by the use of a surveillance device as required by s. 30N(d) of the SD Act

- Errors in recording the details of when protected information is given in evidence as required by s. 30N(e) of the SD Act.

The inspections revealed that the majority of the large number of entries made in PIRs are made correctly. On the whole, records inspected in the period under report demonstrated that investigators had a reasonable understanding of the entries required to be made. However, as set out in Table 1, 33 (73%) of the PIRs containing 'new' entries had at least one error concerning an entry required by s. 30N, and 14 (31%) had both use and communication errors. That is so despite each register containing several pages of clear instructions and sample entries to assist investigators.

It is common for circumstances to arise whereby use and communication of PI occur as a single event. For example, PI obtained pursuant to one surveillance device warrant may be included in an affidavit accompanying an application for a separate surveillance device warrant. This necessarily requires recording both the use of PI (in the compilation of the affidavit) and the external communication of PI (to a judge or magistrate before whom the application for the additional warrant is made). Failing to record the use of PI in such a circumstance will usually result in also failing to record details of the communication. It is in such circumstances that many of the instances of PIRs having both a use and communication error arise.

[29] Comprising 42 PIRs inspected for the first time or where it was expected at a previous inspection that further entries would be made, in addition to the three PIRs re-inspected (due to errors having previously been identified) which also contained 'new' entries.

TABLE 1: PROTECTED INFORMATION REGISTER INSPECTION RESULTS – REGISTERS CONTAINING 'NEW' ENTRIES

Total number of registers containing 'new' entries inspected.	45	100%
Registers without errors.	12	27%
Registers with one or more errors.	33	73%
Registers with a 'use' error (excluding use of PI when given in evidence).	23	51%
Registers with a 'communication' error.	14	31%
Registers with both a use and a communication error.	14	31%
Number of registers with an error in recording PI given in evidence.	6	13%

Inspection of the PIRs suggests that investigators know what details are required to be entered, but on occasion fail to do what is required or to identify omissions or mistakes in the records they have made. It was therefore the SIM's view, with which the VI agrees, that special care and diligence are required by investigators to ensure the accuracy of register entries made pursuant to paras. 30N(c), (d) and (e).

Rectifying previous PIR errors

Of the 17 PIRs re-inspected in the period under report because they had been found at previous inspections to contain errors (omissions or mistakes), there were13 (76%) which, on re-inspection, were found to have been rectified or explained. The four remained unrectified and unexplained errors. The errors had been previously advised by the SIM's inspecting officers to the investigation work unit and to a senior officer after the inspection in which they were identified.

Warrant file records

SPU and ESD maintain records pertaining to each surveillance device or retrieval warrant application, the warrant, and records of emergency authorisations issued.

Inspections by the SIM since 2006 have consistently revealed that administration practices within these units operate effectively and achieve high overall standards of statutory compliance. This has continued to be the case in the period under report.

The SIM, through his inspection officers, reported warrant file inspection results directly to SPU and ESD after each warrant inspection. This was considered valuable by both the agency and the SIM, as it enabled the SIM to receive the response of Victoria Police to any compliance or practice issues identified and allowed the agency to address promptly any matters requiring attention in order to maintain high standards of compliance. The VI agrees that these reports are valuable and proposes to continue them.

Reports pursuant to s. 30K

Notwithstanding the generally high level of compliance, one matter affecting compliance that was repeatedly commented upon by the SIM in reporting under the SD Act was the accuracy of reports made pursuant to s. 30K to the judges and magistrates who issued surveillance device or retrieval warrants.

In drafting such reports, SPU and ESD staff rely upon information received from investigators by way of what the agency refers to as 'Effectiveness Reports'. The s. 30K Report must include, inter alia, 'details of the benefit to the investigation of the use of the device and of the general use made or to be made of any evidence or information obtained by the use of the device'.[30] If the information provided by an Effectiveness Report is incomplete or erroneous, the content of the relevant s. 30K Report is likely to be similarly deficient.

Substantial delay between receipt of the Effectiveness Report and the writing of the s. 30K Report may also result in information not being current. The SIM noted a small number of occasions in the period under report where such delay was significant. (In one instance the s. 30K Report was dated 112 days after the Effectiveness Report.) However, in a number of those cases the SPU team member drafting the report sought an update from the investigators concerned.

[30] Section 30K(2)(viii).

Whilst seeking an update from an investigator may minimise the effect of any delay, the SIM considered, and the VI agrees, that eliminating undue delay in the first instance would likely be the most effective way to ensure matters are accurately reported under s. 30K.

A total of 103 warrant files were inspected in the period under report.[31] Table 2 below summarises the results of inspections of s. 30K Reports conducted in August and December 2012 and divides errors[32] into the following categories:

- Errors in reporting the details of the general use made or to be made of information obtained by use of the device(s) as required by s. 30K(2)(viii) ('use errors')
- Errors in reporting the details of the benefit to the investigation of use of the device(s) as required by s. 30K(2)(viii) ('benefit errors')
- Other errors in relation to information required to be included pursuant to s. 30K of the SD Act.

TABLE 2: ERRORS IN REPORTS UNDER S. 30K

	Warrants ceasing January to April 2012 (August inspection)		**Warrants ceasing May to August 2012 (December inspection)**	
Total Warrants	39		64	
Reports containing Use Errors	1	3%	3	5%
Reports containing Benefit Errors	8	21%	0	0%
Reports containing Other Errors	12	31%	15	23%
Report made on Time	39	100%	64	100%

[31] The total of 103 warrants (39 inspected in August and 64 inspected in December 2012) covers SD and retrieval warrants only. Two emergency authorisations were also inspected but do not have to be reported under the provisions of s. 30K.
[32] As with Table 1, the term 'error' includes both omissions and mistakes.

Table 2 indicates an overall reduction in the percentage of s. 30K Reports containing an error at the December inspection compared with the August inspection. Notably, the percentage of reports containing 'benefit errors' dropped from 21% to zero. 'Use errors' remained low in December at 5% of 64 reports (compared with 3% of 39 reports in August).

A 25% decrease in reports containing 'other' errors (from 31% in August to 23% in December) was also achieved. Such errors concern administrative information that must be included in s. 30K Reports and which is gathered and entered by SPU or ESD registry staff. Because of the nature of these errors, further reduction of them lies substantially in the hands of Victoria Police staff drafting and checking the s. 30K Reports. The errors which are readily identified during the inspection of warrant file documentation by the SIM's inspecting officers should be equally apparent to registry staff.

The SIM acknowledged recent work done (at SPU in particular) in obtaining improved Effectiveness Reports from investigators from which information for the s. 30K reports is obtained. The SIM considered, and the VI agrees, that that focus needs to be maintained, while care should now be taken to reduce further the number of 'other errors' identified in s. 30K Reports.

The SIM noted that all of the s. 30K Reports were made within the time stated in the respective warrants. This result is a notable administrative achievement.

Agency register

Registers of warrants and emergency authorisations kept by SPU and ESD pursuant to the requirements of s. 30O of the SD Act were inspected and found to be generally compliant and up to date. For practical reasons the agency maintains two Registers.

Destruction of records and security of filed records

Inspection of a limited number of documents certifying the destruction of surveillance device records pursuant to ss. 30H(1)(b) and 30N(f) of the SD Act indicated compliance with those provisions.

As noted in previous reports by the SIM, there is some variation in the procedure between SPU and ESD in respect of the handling of residual surveillance device records required by the SD Act to be kept indefinitely.

Residual records for warrants administered by ESD are returned to ESD where they are placed on the warrant file. When ESD warrant files are archived all material is stored in one location which is recorded in the ESD registry records.

The residual records for warrants administered by SPU are filed at various regional police sites. The location of those residual records is notified to SPU by way of documentation relating to the destruction of PI held by investigators. One of the reasons for filing residual records at regional police sites was because there was insufficient space at the SPU premises. While that limitation is acknowledged, the SIM suggested, and the VI agrees, that completed surveillance device warrant files could be safely archived off-site in the one location, as already happens with telecommunications interception warrant files.

In previous reports, the SIM expressed concern in relation to the lack of a reliable central register recording where residual records have been filed by SPU. A central register would assist in ensuring the security of filed records, and make them easier to locate when inspecting officers wish to assess the agency's compliance with paras. 30H(1) and 30N(f) of the SD Act.

The SIM was informed that since the inspection of warrant files in December 2012, SPU has made amendments to a local database used to assist in the management of surveillance device records so that the location of residual records can now be recorded electronically. The location of residual records is now being entered into the database after receipt of the documentation relating to the destruction of PI held by investigators. It remains to be seen whether the location details of records already archived will be recorded in this database also.

SPU's implementation of the process of electronically recording the location of residual surveillance device records filed at designated regional locations is in its infancy and will be of particular interest to the SIM during future inspections.

Use of emergency authorisations

Records of two emergency authorisations were inspected. These concerned the exercise of the emergency authorisation provisions of s. 26 of the SD Act, pursuant to which a senior officer may authorise the use of a surveillance device, without a surveillance device warrant, in prescribed circumstances. Both emergency authorisations inspected related to critical incidents where the senior officer was satisfied that there were reasonable grounds for a suspicion or belief that imminent danger of serious personal violence existed.

In both instances the agency complied with all statutory requirements, including those requiring certain records to be kept and that an application be made within two business days to a Supreme Court judge for approval of the exercise of powers under the emergency authorisation. On both occasions the judge granted approval of the exercise of the emergency powers.

New developments

The SIM noted that a small number of ESD warrants now have electronic PIRs in which investigators make the records required by paras. 30N(c), (d) and (e). A small number of these registers were inspected. The required information was recorded. Some practical aspects of the register format have been discussed with ESD staff, but from a strict compliance perspective the registers achieved the intended purpose.

Summary for Victoria Police

Victoria Police is administering the use of surveillance devices under warrant in a manner generally compliant with the SD Act. The number of issues to report is relatively small, considering the breadth of the statutory framework that must be complied with and the volume of records involved.

Some mistakes and omissions continued to occur in relation to the records that were required to be kept and that were subsequently inspected by the SIM. However an identifiable reduction in errors was achieved in the making of reports to judges and magistrates pursuant to s. 30K of the SD Act and there were indications of some improvement in the accuracy and completeness of record keeping by investigators,

although there was still some scope to improve this to a more satisfactory level through better attention to detail.

As noted above, Victoria Police has, in light of previous comments by the SIM, implemented a procedure for recording the location of residual surveillance device records kept after certain other information has been destroyed in accordance with s. 30H(1)(b). This seeks to address the concerns expressed by the SIM in relation to the security requirements of s. 30H(1)(a) and the ability of the SIM to inspect records in relation to s. 30H(1).

Newly developed electronic PIRs are now in use for warrants administered by ESD. It is too early to determine how effective these will be in meeting the statutory requirement for certain records to be kept. Those inspected so far have met this requirement, but have been tested only in a small number of cases. The SIM noted that consideration was being given by Victoria Police to possible future integration of surveillance device records into the crime investigation management system known as Interpose. How the register development within ESD fits into this program was unclear.

The general level of compliance achieved by Victoria Police during the period under report was high, notwithstanding the issues discussed concerning errors in registers maintained by investigators and in reports made under s. 30K.

NEXT REPORT ON ALL AGENCIES

As required by the SD Act, the next report on the four agencies will be tabled as soon as practicable after 1 July 2013.

Robin Brett, QC

Inspector