

**VICTORIAN
INSPECTORATE**

Inspection Report:

Surveillance Devices Act 1999 (Vic)

Report by the Victorian Inspectorate on surveillance device records inspected during the period 1 January 2021 to 30 June 2021

Contents

Overview	3
Introduction.....	4
OUR ROLE.....	4
HOW WE ASSESS COMPLIANCE	4
HOW WE REPORT ON COMPLIANCE	5
Department of Environment Land Water and Planning.....	6
Game Management Authority.....	7
Independent Broad-based Anti-corruption Commission	8
FINDINGS WARRANTS	8
FINDINGS - RECORDS	9
FINDINGS - REPORTS	10
FINDINGS - TRANSPARENCY AND COOPERATION	11
Victorian Fisheries Authority	13
FINDINGS WARRANTS	13
FINDINGS - RECORDS	14
FINDINGS - REPORTS	15
FINDINGS - TRANSPARENCY AND COOPERATION	16
Victoria Police	17
FINDINGS WARRANTS	17
FINDINGS - RECORDS	18
FINDINGS - REPORTS	19
FINDINGS - TRANSPARENCY AND COOPERATION	20

Overview

This report presents the results of the inspections conducted by the Victorian Inspectorate ('the VI') from 1 January to 30 June 2021 of records belonging to the following five Victorian agencies authorised to use surveillance devices:

- Department of Environment, Land, Water and Planning (DELWP)
- Game Management Authority (GMA)
- Independent Broad-based Anti-corruption Commission (IBAC)
- Victorian Fisheries Authority (VFA)
- Victoria Police

The *Surveillance Devices Act 1999 (Vic)* ('the SD Act') provides the legislative framework for these agencies to use surveillance devices to investigate, or obtain evidence of the commission of, an offence that has been, is being, is about to be, or is likely to be, committed. Law enforcement officers of these agencies can apply to the Supreme Court for a surveillance device warrant with respect to the following types of devices: data; listening; optical; and tracking. For tracking devices only, an application may also be made to the Magistrates' Court. Victoria's Public Interest Monitor (PIM) is entitled to make submissions on warrant applications. In addition to court-issued warrants, senior officers of Victoria Police and IBAC can, in certain emergency situations, authorise the use of surveillance devices.

The role of the VI is established by the SD Act, and ensures independent oversight of the above agencies with respect to compliance with the Act. The VI is required to inspect from time to time the records of each agency and report on the results of its inspections at six-monthly intervals to each House of Parliament as well as the Attorney-General. The use of surveillance devices by Victorian government agencies is highly intrusive, and therefore the VI's role is designed to assure the public that the lawfulness of agency actions is subject to independent checks.

As a result of interruptions to the VI's inspection program in 2020 caused by the COVID-19 pandemic, the inspections of surveillance device records scheduled for the 1 July to 31 December 2020 period were postponed until the inspection period covered by this report. Rather than only deal with records for a six-month period (ordinarily the six months that immediately precedes the inspection period), the inspections conducted from 1 January to 30 June 2021 dealt with records for all of 2020. This report therefore gives findings for warrants that ceased, destruction activity taken and evidentiary certificates issued during the 2020 calendar year. The VI inspected 100% of the records made available at the inspections.

The VI notes in this report the cooperative and transparent engagement by the officers of each agency whose records were subject to our inspection. While the VI reports on some errors, no significant compliance issues were identified. The VI commends the remedial actions taken by the relevant agencies to address the identified errors.

The VI has not made any recommendations as a result of its inspections of surveillance device records for the 1 January to 30 June 2021 reporting period.

Introduction

The SD Act imposes strict controls on the use of surveillance devices by Victorian law enforcement agencies, including the use and communication of information obtained by the use of such devices, and sets out reporting obligations. It also imposes requirements for the secure storage and destruction of records or reports containing information obtained by the use of surveillance devices.

OUR ROLE

The VI performs an independent oversight function to determine the extent of compliance achieved by law enforcement agencies that have exercised their powers under the SD Act.

The VI is required to inspect the records of these agencies from time to time to determine the extent of compliance with the SD Act. In order to fulfil our requirement to report to Parliament at six-monthly intervals, the VI conducts biannual inspections of:

- surveillance device warrants;
- emergency authorisations; and
- retrieval warrants;

which ceased during the preceding 6-month period. As noted in the Overview section, inspection postponements caused by COVID-19 mean the inspections conducted from 1 January to 30 June 2021 dealt with records for all of 2020.

HOW WE ASSESS COMPLIANCE

The VI inspects hard copy documents and electronic registers with the primary purpose of ensuring that records connected with the issue of surveillance device warrants, and other records connected with the use of devices, are being properly kept. The VI will also confirm that each law enforcement agency has met its prescribed reporting obligations. We assess compliance based on the records made available to us at the time of inspection, our discussions with the relevant agencies, as well as the action they take in response to any issues we have raised.

HOW WE REPORT ON COMPLIANCE

To ensure procedural fairness, each agency is given an opportunity to comment on the VI's findings from our inspections and to furnish additional records that might assist our assessment. Following this process, the inspection results are considered finalised.

The report provides detail where there is a finding of non-compliance. The VI may, at its discretion, not report on administrative issues (such as typographical or transposition errors) or instances of non-compliance where the consequences are negligible.

The following sections of this report provide the results of the VI's inspection of surveillance records from 1 January to 30 June 2021. Inspection results are reported on separately for each Victorian law enforcement agency with the authority to exercise powers under the SD Act.

Department of Environment Land Water and Planning

The DELWP's 'Intelligence and Investigations Unit' administers surveillance device warrants issued to the agency.

Since DELWP made no application for a surveillance device warrant during the period covered by this report (1 January to 31 December 2020), the VI did not inspect any DELWP records on this occasion.

Game Management Authority

The GMA has yet to make an application under the SD Act, and as a result no files were inspected by the VI for the period.

Independent Broad-based Anti-corruption Commission

IBAC's 'Legal Compliance Unit' administers surveillance device warrants issued to IBAC. The VI inspected 17 surveillance device files at IBAC on 19 and 25 May 2021, this being all relevant records associated with warrants that ceased between 1 January and 31 December 2020.

FINDINGS WARRANTS

Were applications for warrants (including extensions and variations) properly made?

The VI found that the 17 applications made for a surveillance device warrant by IBAC complied with the requirements of section 15 of the SD Act.

Specifically, the VI found the following requirements were met:

- approval was provided by a senior officer;
- the applicant was a law enforcement officer;
- the applicant's name as well as the nature and duration of the warrant were specified, including the type of device sought;
- a sworn affidavit was provided in support; and
- the application was made to a Supreme Court judge or magistrate, as appropriate.

IBAC also met these requirements in respect of five applications to extend a warrant. Each application was made to a judge in accordance with section 20 of the SD Act.

Were warrants, including retrieval warrants, and emergency authorisations in the proper form, and were revocations properly made?

Issued warrants must specify the following matters in accordance with section 18 of the SD Act:

- the name of the applicant and alleged offence;
- the date warrant was issued, and the kind of surveillance device authorised;
- the premises, object or class of object, or the name of the person (if known) in respect of which the device will be used (as applicable);
- the duration of the warrant (not more than 90 days);
- the name of law enforcement officer primarily responsible for executing the warrant;
- any conditions for the installation or use of the device;
- when the report under section 30K of the SD Act must be made; and
- the name and signature of the issuing authority (magistrate or judge).

All issued surveillance device warrants were found to have met the above-mentioned requirements.

IBAC did not make an application for a retrieval warrant or an emergency authorisation for the use of a surveillance device.

For the inspected warrants, IBAC discontinued the use of surveillance devices and subsequently revoked the associated warrants on seven occasions via written instruments signed by a delegate of the IBAC Commissioner, in accordance with sections 20A and 20B of the SD Act.

FINDINGS - RECORDS

Did IBAC keep all records connected with warrants and emergency authorisations?

IBAC is required to keep records connected with surveillance device warrants in accordance with section 30M of the SD Act, including:

- each warrant issued;
- each emergency authorisation, and application made for such;
- a copy of each warrant application, and any application for its extension, variation or revocation;
- a copy of each application for approval to exercise powers under an emergency authorisation;
- a copy of each report made under section 30K of the SD Act to a magistrate or judge; and
- a copy of each evidentiary certificate issued under section 36 of the SD Act.

IBAC complied with these record-keeping requirements, noting no application was made for an emergency authorisation.

Did IBAC keep all other necessary records?

IBAC is also required to keep other records in accordance with section 30N of the SD Act, including details of:

- each use made of information obtained by the use of a surveillance device;
- each communication of information obtained by the use of a surveillance device to a person other than an IBAC law enforcement officer;
- each occasion information obtained by the use of a surveillance device was given in evidence in a relevant proceeding; and
- the destruction of records or reports obtained by the use of surveillance devices.

The VI found that IBAC complied with these requirements, noting no records or reports were destroyed during the period.

Section 30H(1)(b) of the SD Act requires the IBAC Commissioner to authorise the destruction of information obtained by the use of surveillance devices.

The VI has previously reported that IBAC changed its approval procedure for destroying information under the SD Act. IBAC informed the VI it had decided this approval can be acquitted by the Team

Leader in the Compliance Unit rather than the IBAC Commissioner since this activity is of a reasonably routine administrative nature. Under this implied agency, authorisation to destroy information is made for and on behalf of the IBAC Commissioner.

To ensure the requirements of the SD Act are being satisfied, the VI sought additional information from IBAC, including whether it had considered its ability under s 32(3) of the IBAC Act to delegate this function. In July 2021, IBAC informed the VI it had determined it does have the power to make a delegation and decided, for the avoidance of doubt as to whether its use of implied agency is reasonable, to delegate the power to destroy information obtained by surveillance devices. IBAC further advised the delegation will be progressed immediately and its procedures for dealing with the destruction of records will be amended accordingly. The VI is supportive of these measures and will inspect the delegation instrument and revised procedures at the next scheduled inspection.

Did IBAC maintain an accurate register of warrants and emergency authorisations?

The VI found that IBAC kept a register of warrants, as required by section 30O of the SD Act.

The register specified, with respect to each warrant file inspected, the following particulars:

- the date the warrant was issued;
- the name of magistrate or judge who issued the warrant, as well as the name of the law enforcement officer primarily responsible for its execution;
- the offence in relation to which the warrant was issued;
- the period during which the warrant was in force; and
- any variation or extension of the warrant.

Since IBAC did not exercise its emergency authorisation powers with respect to the inspected files there were no further matters to be specified in the register.

FINDINGS - REPORTS

Were reports to the magistrate and judge properly made?

Under section 30K of the SD Act, IBAC is required, within the time specified in the warrant, to make a report to the magistrate or judge who issued the surveillance device warrant. These reports must state whether the warrant was executed and, if it was, give the following details for its use:

- the name of each person involved in the execution of the warrant;
- the kind of surveillance device used;
- the period the device was used;
- the name of any person whose activities or conversations were captured by use of the device or whose geographic location was determined by the use of a tracking device, if known;
- the premises for installation of the device or the location for its use, as applicable;

- the object in or on which the device was installed or the premises at which the object was located when the device was installed, as applicable;
- the benefit to the investigation of the use of the device as well as the general use made or to be made of the information derived from its use;
- compliance with any warrant conditions, as applicable;
- if the warrant was extended or varied, the number of such occurrences and the reasons for them; and
- if the warrant was revoked by the chief officer under section 20A(2), the reasons the device was no longer required and whether the Public Interest Monitor was notified of the revocation.

The 17 reports made by IBAC for warrants that ceased between 1 January and 31 December 2020 were made within the requisite timeframe and complied with the above-mentioned requirements.

FINDINGS - TRANSPARENCY AND COOPERATION

The VI considers an agency's transparency, its cooperation during inspection, and its responsiveness to suggestions and issues to be a measure of its compliance culture.

Did IBAC self-disclose compliance issues?

IBAC made three self-disclosures at the inspection during the period. These self-disclosures, connected with assistance orders made under section 22 of the SD Act, were brought to the VI's attention prior to the VI commencing its inspection of the relevant records. In all three cases, the approval given by the judge was not made in the proper form. While the form used by IBAC for each assistance order was signed by the judge and specified all matters under section 22(4) of the SD Act, the assistance orders were not endorsed on the face of the relevant surveillance device warrant in accordance with this section.

The VI was informed by IBAC that at the time these assistance orders were made by the Supreme Court, the Court made no comment with respect to section 22(4) requirements. In response to these errors, IBAC advised that it will amend its surveillance device warrant procedures to ensure any future assistance orders are made in the correct form. The VI will inspect these changes at its next scheduled inspection of IBAC records

Were issues identified at previous inspections addressed?

Since no issues with IBAC files were identified from the VI's previous inspection of surveillance device records, there were no historical issues to be addressed on this occasion.

The VI notes that IBAC was responsive and transparent during the inspection process. Although no compliance issues were identified from the inspection, IBAC agreed to make the following process changes in response to feedback from the VI: to amend the section 30K report template to include

OFFICIAL

the relevant warrant reference number; and to include the particular warrant number in emails sent to the Court for transmitting these reports. These changes will make it clear to which warrant each email and report relates.

Victorian Fisheries Authority

The VI inspected two surveillance device files at the VFA on 9 March 2021, these being all relevant records associated with warrants that ceased between 1 January and 31 December 2020.

FINDINGS WARRANTS

Were applications for warrants (including extensions and variations) properly made?

The VI found that the two applications made by the VFA for a surveillance device warrant complied with the requirements of section 15 of the SD Act.

Specifically, the VI found the following requirements were met:

- approval was provided by a senior officer;
- the applicant was a law enforcement officer;
- the applicant's name as well as the nature and duration of the warrant were specified, including the type of device sought;
- a sworn affidavit was provided in support; and
- the application was made to a Supreme Court judge or magistrate, as appropriate.

The VFA made no application under section 20 of the SD Act for a warrant to be extended or varied during the period.

Were warrants, including retrieval warrants in proper form and revocations properly made?

Issued warrants must specify the following matters in accordance with section 18 of the SD Act:

- the name of the applicant and alleged offence;
- the date warrant was issued, and the kind of surveillance device authorised;
- the premises, object or class of object, or the name of the person (if known) in respect of which the device will be used (as applicable);
- the duration of the warrant (not more than 90 days);
- the name of law enforcement officer primarily responsible for executing the warrant;
- any conditions for the installation or use of the device;
- when the report under section 30K of the SD Act must be made; and
- the name and signature of the issuing authority (magistrate or judge).

The two warrants issued to the VFA met all of these requirements.

The VFA did not make an application for a retrieval warrant during the period.

For the inspected warrants, the VFA discontinued the use of a surveillance device and subsequently revoked the associated warrant on one occasion via a written instrument signed by the CEO, in accordance with sections 20A and 20B of the SD Act.

FINDINGS - RECORDS

Did the VFA keep all records connected with warrants?

The VFA is required to keep records connected with surveillance device warrants in accordance with section 30M of the SD Act, including:

- each warrant issued;
- a copy of each warrant application, and any application for its extension, variation or revocation;
- a copy of each report made under section 30K of the SD Act to a magistrate or judge; and
- a copy of each evidentiary certificate issued under section 36 of the SD Act.

The VFA complied with these record-keeping requirements.

Did the VFA keep all other necessary records?

The VFA is also required to keep other records in accordance with section 30N of the SD Act, including details of:

- each use made of information obtained by the use of a surveillance device;
- each communication of information obtained by the use of a surveillance device to a person other than a law enforcement officer of the VFA;
- each occasion information obtained by the use of a surveillance device was given in evidence in a relevant proceeding; and
- the destruction of records or reports obtained by the use of surveillance devices.

The VI found that the VFA complied with these requirements.

Did the VFA maintain an accurate register of warrants?

The VI found that the VFA kept a register of warrants, as required by section 30O of the SD Act.

The register specified, with respect to each warrant file inspected, the following particulars:

- the date the warrant was issued;
- the name of magistrate or judge who issued the warrant, as well as the name of the law enforcement officer primarily responsible for its execution;
- the offence in relation to which the warrant was issued;
- the period during which the warrant was in force; and
- any variation or extension of the warrant.

FINDINGS - REPORTS

Were reports to the magistrate and judge properly made?

Under section 30K of the SD Act, the VFA is required, within the time specified in the warrant, to make a report to the magistrate or judge who issued the surveillance device warrant. These reports must state whether the warrant was executed; and if it was, to give the following details for its use:

- the name of each person involved in the execution of the warrant;
- the kind of surveillance device used;
- the period the device was used;
- the name of any person whose activities or conversations were captured by use of the device or whose geographic location was determined by the use of a tracking device, if known;
- the premises for installation of the device or the location for its use, as applicable;
- the object in or on which the device was installed or the premises at which the object was located when the device was installed, as applicable;
- the benefit to the investigation of the use of the device as well as the general use made or to be made of the information derived from its use;
- compliance with any warrant conditions, as applicable;
- if the warrant was extended or varied, the number of such occurrences and the reasons for them; and
- if the warrant was revoked by the chief officer under section 20A(2), the reasons the device was no longer required and whether the Public Interest Monitor was notified of the revocation.

The two reports made by the VFA for warrants that ceased between 1 January and 31 December 2020 were made within the requisite timeframe, however both reports were found to contain one or more errors.

Finding 1 – Incorrect information given in the report to the judge/magistrate.

Section 30K(2)(b)(iii) of the SD Act requires the report to the magistrate to give the period during which the device was used. In the case of one warrant, the action report made by Victoria Police's Technical Surveillance Unit (TSU) shows the device was installed by its operatives on 7 January 2020, however the report to the magistrate reports instead when the device was *authorised* from – being 19 December 2019.

An error with reporting the period during which the devices were used was repeated in the other warrant file inspected. In this case, the TSU action report showed the last device was retrieved on 5 June 2020, however the VFA's report to the judge instead reported the end date for the authorisation of the devices – being 10 June 2020, the date the warrant was revoked. For the same warrant, a further error was identified with respect to reporting the

operatives involved in the execution of the warrant. The operatives listed in the report to the judge are different to the operatives given in the TSU action reports.

In our follow-up discussions with the VFA, it was confirmed the section 30K report template used by the VFA incorrectly refers to the warrant's authorisation date, rather than the period during which the device is used. The VFA advised that supplementary reports will be made under section 30K of the SD Act to correct the reporting errors. To ensure no re-occurrence of these issues, the VFA further stated it has amended its section 30K report template and has also updated its procedures. The VI will inspect the supplementary reports and procedural changes at the next scheduled inspection.

FINDINGS - TRANSPARENCY AND COOPERATION

The VI considers an agency's transparency, its cooperation during inspection, and its responsiveness to suggestions and issues to be a measure of its compliance culture.

Did the VFA self-disclose compliance issues?

The VFA did not make any self-disclosures relevant to the warrant files inspected from 1 January to 30 June 2021.

Were issues identified at previous inspections addressed?

The VI was not required to inspect any VFA files from the previous inspection of surveillance device records as there were no historical issues to be addressed on this occasion.

The VI notes that the VFA was responsive and transparent during the inspection process. In response to the issues raised by the VI about the reports made to the judge and magistrate, the VFA committed itself to make supplementary reports and amend procedures. The VFA further demonstrated its responsiveness to feedback from the VI by agreeing to amend its use and communications register template so that it explicitly refers to any external agency to which the VFA has communicated information that was obtained by a device.

Victoria Police

There are two units within Victoria Police that administer surveillance device warrants and emergency authorisations:

- Special Projects Unit (SPU), the major user of surveillance device warrants; and
- Technical Projects Unit (TPU), within Professional Standards Command (PSC).

In addition to these units, the TSU within Victoria Police is responsible for the installation, maintenance and retrieval of surveillance devices under the authority of warrants or emergency authorisations. A representative sample of records held by the TSU in relation to these matters were inspected on 27 May 2021 and cross-checked against records held by the SPU and TPU.

The VI inspected all surveillance device files made available for inspection by Victoria Police's SPU and TPU during the period. In total, 72 warrant files were inspected. This includes six warrants that were extended and two occasions a warrant was varied. No application for a retrieval warrant or an emergency authorisation was made during the 2020 calendar year.

Three surveillance device files at the TPU were inspected on 12 May 2021, and 69 files at the SPU were inspected from 15-17 June 2021.

FINDINGS WARRANTS

Were applications for warrants (including extensions and variations) properly made?

The VI found that all applications made for a surveillance device warrant complied with the requirements of section 15 of the SD Act.

Specifically, the VI found the following requirements were met:

- approval was provided by an authorised police officer;
- the applicant was a law enforcement officer;
- the applicant's name as well as the nature and duration of the warrant were specified, including the type of device sought;
- a sworn affidavit was provided in support; and
- the application was made to a Supreme Court judge or magistrate, as appropriate.

In addition to meeting these requirements, Victoria Police made a total of eight applications to extend or vary a warrant – each was made to the judge as required by section 20 of the SD Act.

Were warrants, including retrieval warrants, and emergency authorisations in proper form and revocations properly made?

Issued warrants must specify the following matters in accordance with section 18 of the SD Act:

- the name of the applicant and alleged offence;
- the date warrant was issued, and the kind of surveillance device authorised;
- the premises, object or class of object, or the name of the person (if known) in respect of which the device will be used (as applicable);
- the duration of the warrant (not more than 90 days);
- the name of law enforcement officer primarily responsible for executing the warrant;
- any conditions for the installation or use of the device;
- when the report under section 30K of the SD Act must be made; and
- the name and signature of the issuing authority (magistrate or judge).

The 72 warrants issued to Victoria Police complied with these requirements.

For the inspected warrants, Victoria Police discontinued the use of surveillance devices and subsequently revoked the associated warrants on 59 occasions via written instruments signed by a delegate of the Chief Commissioner of Police, in accordance with sections 20A and 20B of the SD Act.

Victoria Police did not make an application for a retrieval warrant, nor did it make any emergency authorisations for the use of a surveillance device in the period.

FINDINGS - RECORDS

Did Victoria Police keep all records connected with warrants and emergency authorisations?

Victoria Police is required to keep records connected with surveillance device warrants in accordance with section 30M of the SD Act, including:

- each warrant issued;
- each emergency authorisation, and application made for such;
- a copy of each warrant application, and any application for its extension, variation or revocation;
- a copy of each application for approval to exercise powers under an emergency authorisation;
- a copy of each report made under section 30K of the SD Act to a magistrate or judge; and
- a copy of each evidentiary certificate issued under section 36 of the SD Act.

Victoria Police complied with these record-keeping requirements, noting no application was made for an emergency authorisation. A total of 43 evidentiary certificates were inspected for the period.

Did Victoria Police keep all other necessary records?

Victoria Police is also required to keep other records in accordance with section 30N of the SD Act, including details of:

- each use made of information obtained by the use of a surveillance device;

- each communication of information obtained by the use of a surveillance device to a person other than a Victoria Police law enforcement officer;
- each occasion information obtained by the use of a surveillance device was given in evidence in a relevant proceeding; and
- the destruction of records or reports obtained by the use of surveillance devices.

The VI found that Victoria Police complied with these requirements. The VI identified an error in the information recorded in the electronic register about the use made of information obtained by a surveillance device for one warrant. Victoria Police's SPU confirmed that the information it had reported to the judge under section 30K of the SD Act correctly recorded the use that was made and amended the electronic register accordingly.

Victoria Police kept details on the destruction of records and reports related to 73 surveillance device warrants in accordance with section 30N(f) of the SD Act.

Did Victoria Police maintain an accurate register of warrants and emergency authorisations?

The VI found that Victoria Police kept a register of warrants, as required by section 30O of the SD Act.

The register specified, with respect to each warrant file inspected, the following particulars:

- the date the warrant was issued;
- the name of magistrate or judge who issued the warrant, as well as the name of the law enforcement officer primarily responsible for its execution;
- the offence in relation to which the warrant was issued;
- the period during which the warrant was in force; and
- any variation or extension of the warrant.

Since Victoria Police did not exercise its emergency authorisation powers with respect to the inspected files there were no further matters to be specified in the register.

FINDINGS - REPORTS

Were reports to the magistrate and judge properly made?

Under section 30K of the SD Act, Victoria Police is required, within the time specified in the warrant, to make a report to the magistrate or judge who issued the surveillance device warrant. These reports must state whether the warrant was executed; and if it was, to give the following details for its use:

- the name of each person involved in the execution of the warrant;
- the kind of surveillance device used;
- the period the device was used;

- the name of any person whose activities or conversations were captured by use of the device or whose geographic location was determined by the use of a tracking device, if known;
- the premises for installation of the device or the location for its use, as applicable;
- the object in or on which the device was installed or the premises at which the object was located when the device was installed, as applicable;
- the benefit to the investigation of the use of the device as well as the general use made or to be made of the information derived from its use;
- compliance with any warrant conditions, as applicable;
- if the warrant was extended or varied, the number of such occurrences and the reasons for them; and
- if the warrant was revoked by the chief officer under section 20A(2), the reasons the device was no longer required and whether the Public Interest Monitor was notified of the revocation.

All reports made by Victoria Police in accordance with section 30K of the SD Act for warrants that ceased between 1 January and 31 December 2020 were made within the requisite timeframe, however two reports contained an error.

Finding 1 – Incorrect information given in the report to the judge.

In one warrant file, the TSU action report shows a particular operative conducted maintenance on an installed device on multiple occasions, however the report to the judge does not list this operative as being involved in the execution of the warrant as required by section 30K(2)(b)(i) of the SD Act.

In one other file, although the TSU action report shows a device was installed on 17 January 2020, the report to the judge with respect to section 30K(2)(b)(iii) of the SD Act states the same device was used from 16 January 2020, which was the date when the warrant was issued.

Victoria Police's SPU confirmed the discrepancies were caused by errors made in the reports to the judge and further advised supplementary reports had been made to correct these inaccuracies. The VI will inspect these additional reports at the next scheduled inspection.

FINDINGS - TRANSPARENCY AND COOPERATION

The VI considers an agency's transparency, its cooperation during inspection, and its responsiveness to suggestions and issues to be a measure of its compliance culture.

Did Victoria Police self-disclose compliance issues?

Victoria Police's SPU made one self-disclosure at the inspection during the period. A supplementary report was made to the judge under section 30K of the SD Act to report that information obtained by use of a device was used in an application for a prospective information authorisation.

Victoria Police also informed the VI of a change made in 2020 to the Supreme Court's process for delivering an issued surveillance device warrant to the applicant in cases where the applicant is not required to attend a hearing. The change to allow the delivery of a warrant electronically - made in response to the COVID-19 pandemic – means the warrant kept on file in accordance with section 30M(a) of the SD Act may be a print-out of the electronic copy rather than the original signed version.

Were issues identified at previous inspections addressed?

The VI partially re-inspected one warrant file from the previous inspection of records at Victoria Police's SPU. The VI confirmed that a copy of the section 30K report was made to the magistrate who issued the surveillance device warrant.