Integrity Oversight Victoria

OCTOBER 2025

Surveillance Devices Inspection Report

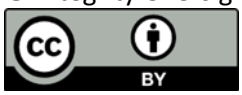
Report by Integrity Oversight Victoria on its inspections of surveillance device records during the period
1 January 2024 to 30 June 2024

Integrity Oversight Victoria
Level 8, 565 Bourke Street
Melbourne VIC 3000

Telephone: 1800 518 197
integrityoversight.vic.gov.au

Acknowledgement
Integrity Oversight Victoria acknowledges Aboriginal and Torres Strait Islander people as the Traditional Custodians of Country. We respectfully acknowledge all First Peoples of Victoria and celebrate their enduring connection to land, skies and waters. We thank First Peoples for their care of Country and contributions to Victorian communities. We honour and pay our respects to First Peoples' Elders past and present.

Published by order, or under the authority, of the Parliament of Victoria, October 2025.



ISSN 2982-2912 (online)
Published October 2025

If you would like to receive this information in a more accessible format, please call 1800 518 197 or email communications@integrityoversight.vic.gov.au. This document is also available at integrityoversight.vic.gov.au.

Contents

Overview

This report presents the results of inspections conducted by Integrity Oversight Victoria from 1 January to 30 June 2024 for Victorian agencies authorised to use surveillance devices. Since our biannual inspections deal with warrants that ceased during the preceding 6-month period, this report gives findings for records relevant to the 1 July to 31 December 2023 period – the 'reporting period'.

We inspected 100% of the records available for inspection.

The following 6 agencies[1] were authorised to exercise surveillance device powers during the reporting period:

- Department of Energy, Environment and Climate Action (DEECA)
- Environment Protection Authority (EPA)
- Game Management Authority (GMA)
- Independent Broad-based Anti-corruption Commission (IBAC)
- Victorian Fisheries Authority (VFA)
- Victoria Police.

The EPA and GMA were the only agencies that did not exercise their powers under the *Surveillance Devices Act 1999* (Vic) (the SD Act) during this period.

This report details some compliance errors identified at our regular inspections of surveillance device records during the 1 January to 30 June 2024 period. While we made some suggestions with respect to errors we identified and other errors disclosed to us by oversighted agencies, we did not make any recommendations from our inspections during this period.

The SD Act provides the legislative framework for relevant 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 authorising use of the following types of devices: data, listening, optical, and tracking. For tracking devices only, an application may be made to the Magistrates' Court. In addition to court-issued warrants, senior officers of Victoria Police and IBAC can in certain emergency situations, authorise the use of surveillance devices.

Victoria's Public Interest Monitor (PIM) is entitled to make submissions on warrant applications.

Our role is established by the SD Act, to provide independent oversight of agencies' compliance with the SD Act. We are required to inspect, from time to time, the records of each agency and report on the results of our inspections at 6-monthly intervals to each House of Parliament as well as the responsible Minister (Attorney-General). These 6-monthly inspections constitute our regular inspection framework. The use of surveillance devices by Victorian government agencies is a serious intrusion on a person's right to privacy, and it is our role to assure the public that the administration of surveillance devices is subject to independent checks.

[1] While the Office of the Special Investigator was not abolished by legislation until 2 February 2024, as previously reported, its investigative and analytical functions ceased on 27 June 2023.

This report gives the results from our inspection of warrants at DEECA, IBAC, VFA, and Victoria Police that ceased during the reporting period, and any warrant applications refused, destruction activity undertaken and evidentiary certificates issued during the same period.

For the EPA and GMA, we received confirmation from each that they had no ceased warrants or other surveillance device records for the reporting period. As a result, we did not conduct an inspection at these agencies on this occasion.

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 from such devices. It also imposes reporting obligations, and requirements for the secure storage and destruction of records and reports containing information obtained by their use.

Our role

Integrity Oversight Victoria provides independent oversight by inspecting the records of law enforcement agencies to determine the extent of their compliance with the SD Act.

To fulfil our requirement to report to Parliament at 6-monthly intervals, we conduct biannual inspections of surveillance device warrants, emergency authorisations and retrieval warrants which ceased during the preceding 6-month period.

How we assess compliance

We inspect hard-copy and electronic documents for the primary purpose of ensuring that records about the issue of surveillance device warrants, and other records about the use of any surveillance device, are properly made and kept. We 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 agency, and the action they take in response to any issues we raise.

How we report on compliance

To ensure procedural fairness, each agency is given an opportunity to comment on inspection findings and to furnish additional records that may assist our assessment. Following this process, the inspection results are considered finalised. Each agency is also provided relevant extracts of our draft report for comment.

The report provides detail where there is a finding of non-compliance. We may, at our 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 Integrity Oversight Victoria's inspection of surveillance records during the period 1 January to 30 June 2024. Inspection results are separately reported for each Victorian law enforcement agency which exercised powers under the SD Act in the reporting period.

Department of Energy, Environment and Climate Action

DEECA's surveillance device warrants are administered by its Strategic Operations and Intelligence Unit. On 13 June 2024, we conducted an inspection of the 3 surveillance device warrants issued to DEECA. For each warrant, we identified an error with the information reported to the issuing judge.

We also inspected records connected to 2 withdrawn applications for a surveillance device warrant. Together with the issued warrants, these represented all eligible surveillance device records for the 6-month period ending 31 December 2024.

Findings: warrants

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

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

Specifically, we found the following requirements were met:

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

We also inspected records connected with 2 applications for a surveillance device warrant that did not proceed. Although approval was given for these applications, they were withdrawn prior to the scheduled hearing.

While we found no concerns with these withdrawn applications, DEECA's process for assigning a reference number to applications and warrants resulted in a discrepancy with information recorded in its register of warrants. Although this register records each application in sequential order from when it was made, applications and warrants are otherwise identified on the basis of the number of warrants issued to DEECA for the year. On one occasion we found an application, and the resultant warrant, was identified by a number that was allocated to a withdrawn application. To avoid potential confusion and ensure the records correlate with information kept in the register of warrants, we suggested the reference number should stay with an application irrespective of whether it resulted in an issued warrant.

For the inspected records, DEECA did not apply to extend or vary a warrant under section 20 of the SD Act.

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

Issued surveillance device 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 the 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 the 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
- the name and signature of the issuing authority (magistrate or judge).

The 3 warrants issued to DEECA met all these requirements.

DEECA did not apply for a retrieval warrant during the period.

For each inspected warrant, DEECA discontinued the use of a surveillance device and sought to revoke the warrant. Although the Secretary of the Department signed a written instrument to revoke each warrant, this was done 2 days after the warrants had already expired.

To support DEECA's compliance with sections 20A and 20B of the SD Act, we suggested that in cases where it decides a surveillance device is no longer required, approval for the warrant's revocation be sought at least 2 full business days prior to its expiry. This will ensure DEECA can obtain approval to revoke a warrant that is no longer required before it expires. We further suggested the briefing note that accompanies the instrument explicitly inform the delegate of the date by which the instrument must be signed. We subsequently confirmed at the next inspection that DEECA had revised its brief to the Secretary, so it clearly identifies the warrant's expiry date.

Findings: records

Did DEECA keep all records connected with warrants?

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

- each warrant issued
- each notice given under section 20A(3) for the revocation of a warrant
- 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
- a copy of each evidentiary certificate issued under section 36 of the SD Act.

DEECA complied with these record-keeping requirements with respect to the 3 warrants for the reporting period. We were informed that DEECA did not make any evidentiary certificates connected to a surveillance device warrant during the same period.

Did DEECA keep all other necessary records?

DEECA must also 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 DEECA law enforcement officer
- each occasion information obtained by the use of a surveillance device was given in evidence in a relevant proceeding
- the destruction of records or reports obtained by the use of surveillance devices.

We found that DEECA complied with these requirements, noting no records or reports were destroyed during the reporting period.

Did DEECA maintain an accurate register of warrants?

We found that DEECA kept a register of warrants, as required by section 30O of the SD Act.

The register is to specify the following particulars for each surveillance device warrant:

- the date the warrant was issued
- the name of the magistrate or judge who issued the warrant, and 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
- any variation or extension of the warrant.

DEECA complied with these requirements, except in respect of specifying the offences under the *Forests Act 1958* in relation to which the warrants were issued. We found at the next inspection that DEECA had amended its register of warrants template to reflect this feedback.

Findings: reports

Were reports to the magistrate or judge properly made?

Under section 30K of the SD Act, DEECA is required, within the time specified in the warrant, to report to the magistrate or judge who issued the 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 at which the device was installed or the location of 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
- if the warrant was revoked by the chief officer under section 20A(2) of the SD Act, the reason the device was no longer required and whether the PIM was notified of the revocation.

While the reports made by DEECA for the 3 inspected warrants were made within the requisite timeframe, each report was found to contain a reporting error.

Finding: incorrect information given in the 3 reports to the judge

DEECA must report to the judge who issued the warrant, among other things, the name of each person[2] who was involved in the execution of the warrant. For the warrants it is issued with, DEECA depends on the expertise of Victoria Police's Technical Surveillance Unit (TSU) to execute their warrants. For the 3 warrants, we found each report to the judge identified one or more persons as having executed the warrant that were not recorded in the action report sheets made by Victoria Police's TSU for the same warrant.

Enquiries with DEECA confirmed this discrepancy was caused by including persons who prepared the TSU reports but were otherwise not involved in execution of the warrant in the reports made under section 30K of the SD Act. In response to our suggestion that it make amended reports, we later confirmed that DEECA corrected these errors in 3 supplementary reports given to the issuing judge.

Findings: transparency and cooperation

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

During our post-inspection enquiries, we suggested to DEECA that it make supplementary reports under section 30K of the SD Act and changes to its procedures for administering surveillance device warrants. We confirmed at the next inspection that DEECA made correction reports and had also revised its register of warrants as well as a briefing template for seeking approval from the Secretary to revoke a warrant.

Did DEECA self-disclose compliance issues?

DEECA did not make any self-disclosures at the inspections conducted during the period.

[2] In an email from September 2023, the Supreme Court confirmed that with respect to being notified of the persons involved in the execution of a warrant, the report may give the operative's unique number rather than their name.

Were issues identified at previous inspections addressed?

There were no historical issues to be addressed at this inspection. Noting DEECA's infrequent use of its powers under the SD Act, our previous inspection of DEECA surveillance device records was conducted in the 1 July to 31 December 2019 inspection period.

Independent Broad-based Anti-corruption Commission

IBAC's Internal Compliance team administers surveillance device warrants issued to IBAC. On 8 May 2024, we conducted an inspection of one surveillance device warrant issued to IBAC. No issues were identified with this warrant. We also inspected records connected to the destruction of 3 surveillance device warrants. These represented all eligible surveillance device records for the 6-month period ending 31 December 2023.

Findings: warrants

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

We found the application for a surveillance device warrant made by IBAC complied with the requirements of section 15 of the SD Act.

Specifically, we found the following requirements were met:

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

For the one inspected warrant, IBAC did not make an application to either extend or vary the warrant.

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

Issued surveillance device 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 the 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 the 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

- the name and signature of the issuing authority (magistrate or judge).

IBAC did not make an application for a retrieval warrant or for an emergency authorisation to use a surveillance device during the reporting period. IBAC did not revoke a warrant via a written instrument signed by a delegate of the IBAC Commissioner.

Findings: records

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

IBAC must keep records connected with warrants and emergency authorisations in accordance with section 30M of the SD Act, including:

- each warrant issued
- each notice given under section 20A(3) for the revocation of a warrant
- 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
- a copy of each evidentiary certificate issued under section 36 of the SD Act.

IBAC complied with these record-keeping requirements for the reporting period. We were informed that IBAC did not make any evidentiary certificates connected to a surveillance device warrant during the same period.

Did IBAC keep all other necessary records?

IBAC must also 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 officer
- each occasion information obtained by the use of a surveillance device was given in evidence in a relevant proceeding
- the destruction of records or reports obtained by the use of surveillance devices.

We found that IBAC complied with these requirements and kept details on the destruction of records and reports related to 3 surveillance device warrants in accordance with section 30N(f) of the SD Act.

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

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

The register specified the following particulars for the inspected surveillance device warrant:

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

Since IBAC did not exercise its emergency authorisation powers during the relevant period, there were no matters to be specified in the register in relation to section 30O(3) of the SD Act.

Findings: reports

Were reports to the magistrate or 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 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 at which the device was installed or the location of 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
- if the warrant was revoked by the chief officer under section 20A(2) of the SD Act, the reason the device was no longer required and whether the PIM was notified of the revocation.

The report made by IBAC under section 30K of the SD Act complied with these requirements and was made within the requisite timeframe.

Findings: transparency and cooperation

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

During our post-inspection enquiries, we noted that a revised email template used by IBAC to notify its investigators of the issue of a surveillance device warrant incorrectly informed investigators that in cases where the grounds for the use of the authorised device(s) no longer exist the warrant "should", rather than *must*, be revoked. Under sections 20A and 20B of the SD Act, IBAC must revoke a warrant once it determines the use of the authorised device(s) is no longer necessary to ensure the impact on individual privacy is limited. We subsequently confirmed at the next inspection that IBAC had revised its warrant notification email template to align with this requirement.

Did IBAC self-disclose compliance issues?

IBAC did not make any self-disclosures at the inspection conducted during the period.

Were issues identified at previous inspections addressed?

We previously reported that IBAC made a supplementary report under section 30K of the SD Act to notify the issuing judge of an irregularity between the warrant particulars and the type of composite surveillance device that was installed and used. This supplementary report was inspected by us at the May 2024 inspection.

IBAC disclosed at our previous inspection that the report it made under section 30K of the SD Act for one warrant omitted a use made of information obtained by the authorised surveillance device due to a back-dated entry in the use and disclosure register. We confirmed at the May 2024 inspection that IBAC made a supplementary report to the issuing judge that included this additional information.

Victorian Fisheries Authority

On 27 March 2024, we inspected the 2 surveillance device warrants issued to the VFA during the reporting period. For one of these warrants, we found the report made under section 30K of the SD Act incorrectly reported the period during which the authorised surveillance device was used.

We also inspected records connected to the revocation of one warrant. These represented all eligible surveillance device records for the 6-month period ending 31 December 2023.

Findings: warrants

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

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

Specifically, we found the following requirements were met:

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

For the inspected records, the VFA did not apply to extend or vary a warrant under section 20 of the SD Act.

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

Issued surveillance device 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 the 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 the 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
- the name and signature of the issuing authority (magistrate or judge).

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

The VFA did not apply for a retrieval warrant during the period.

For one warrant, the VFA discontinued the use of the surveillance device and subsequently revoked the associated warrant 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 must keep records connected with warrants in accordance with section 30M of the SD Act, including:

- each warrant issued
- each notice given under section 20A(3) for the revocation of a warrant
- 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
- a copy of each evidentiary certificate issued under section 36 of the SD Act.

The VFA complied with these record-keeping requirements in relation to the inspected warrants. We were informed the VFA did not make any evidentiary certificates connected to a surveillance device warrant during the reporting period.

Did the VFA keep all other necessary records?

The VFA must also 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 VFA law enforcement officer
- each occasion information obtained by the use of a surveillance device was given in evidence in a relevant proceeding
- the destruction of records or reports obtained by the use of surveillance devices.

We found the VFA complied with these requirements, noting no records or reports were destroyed during the reporting period.

Did the VFA maintain an accurate register of warrants?

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

The register is to specify the following particulars for each surveillance device warrant:

- the date the warrant was issued
- the name of the magistrate or judge who issued the warrant, and the name of the law enforcement officer primarily responsible for its execution
- the offence for which the warrant was issued
- the period during which the warrant was in force

- any variation or extension of the warrant.

The VFA complied with these requirements.

Findings: reports

Were reports to the magistrate or 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 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 at which the device was installed or the location of 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
- if the warrant was revoked by the chief officer under section 20A(2) of the SD Act, the reason the device was no longer required and whether the PIM was notified of the revocation.

While both reports made by the VFA were made within the requisite timeframe, one report was found to contain a reporting error.

Finding: incorrect information given in the report to the judge for one warrant

Under section 30K(2)(b)(iii) of the SD Act, the report to the judge or magistrate who issued the warrant must state the period during which the authorised device was used. In the case of one warrant, the information in the report to the issuing magistrate did not align with the information given by the technical operatives involved in the execution of the warrant.

Enquiries with the VFA confirmed the section 30K report to the relevant magistrate incorrectly reported the date on which the warrant was revoked rather than when use of the device ceased.

In response to the findings we communicated during the inspection exit interview, the VFA provided us with a revised section 30K report template that included additional instructions to lessen the likelihood of a recurrence of this issue. We suggested various other changes to the template to further strengthen the VFA's ability to meet its reporting obligations.

In our post-inspection enquiries, the VFA provided a further updated reporting template that reflects all the changes we suggested.

In addition to changes to the reporting template, we also made a suggestion for how the VFA provides confirmation of when the section 30K report is delivered to the judge or magistrate who issued the warrant. We note the VFA accepted our suggestion by including explanatory notes in its reporting template.

Findings: transparency and cooperation

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

At the March 2024 inspection we inspected further updates the VFA made to its procedures for administering surveillance device warrants. These changes include improved quality assurance for functions such as making an application, reviewing the use of a device, and seeking the retrieval of a device and revocation of the associated warrant.

The VFA's response to further updates we suggested to their policies and procedures is dealt with in the below section.

Did the VFA self-disclose compliance issues?

The VFA self-disclosed 3 compliance matters at the inspection. These are summarised as follows:

1. Incorrectly sworn affidavit**:** the first sworn affidavit in one warrant application was found invalid by the court. The VFA corrected the error in the affidavit that was later used to support the application for a warrant.
2. Incorrect form of warrant**:** a warrant issued on 3 November 2023 was given an end date of 31 January 2023, rather than 31 January 2024. The VFA disclosed this error to the issuing authority 10 days later and the warrant was amended to show the end date in 2024. The VFA later identified and disclosed to the same authority that the issued warrant incorrectly stated the date on which the application was made.
3. Errors with application documents**:** in a supplementary sworn affidavit made 7 weeks after the warrant was issued, the VFA disclosed to the issuing authority that the exhibit purported to be the sworn affidavit used in the application for the previous warrant was instead an invalid affidavit (the incorrectly sworn affidavit referred to above at item 1). Additionally, the affidavit gave the incorrect location for where the affidavit connected to the previous warrant was sworn; an error repeated in the certificate identifying the exhibit.

With respect to these self-disclosed matters, we suggested the VFA document in policy and procedures the responsible officers for conducting quality assurance checks on an affidavit made in support of an application for a surveillance device warrant. These checks should also extend to the draft warrant prior to it being submitted to the court and the subsequently issued warrant. This will enable any errors to be identified and rectified prior to the VFA executing a warrant.

In response to these suggestions, the VFA provided us with revised procedures that mandate checks of signed documents before a warrant is executed and before a warrant is extended or revoked. We note the VFA's receptiveness to the suggested improvements, and we look forward to working with the VFA in future inspections to further strengthen its documented processes.

Were issues identified at previous inspections addressed?

Other than confirming a change to the VFA's procedures for administering surveillance device warrants, there were no other issues to be addressed from the previous inspection.

Victoria Police

There are 2 units within Victoria Police that administer surveillance device warrants and emergency authorisations:

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

In addition, the Technical Surveillance Unit (TSU) within Victoria Police is responsible for the installation, maintenance, and retrieval of surveillance devices under the authority of warrants or emergency authorisations. Records held by the TSU are inspected annually and cross-checked against records held by the SPU and TPU. TSU records for surveillance warrants that ceased during calendar year 2023 were inspected on 4 June 2024.

We inspected all 34 surveillance device files administered by Victoria Police's SPU and TPU. This includes 31 issued warrants, 2 warrants that were extended, and one that was varied. In addition to records on the destruction of 36[3] surveillance device warrants, we also inspected 13 evidentiary certificates. Altogether, these represent all relevant surveillance device records for the reporting period.

Two surveillance device files at the TPU were inspected on 2 May 2024, and 32 files at the SPU were inspected from 14-16 May 2024.

No issues were identified for the inspected records.

For the total number of warrants granted to Victoria Police for the period, 3 were not executed – representing just under 10% of all issued warrants. It is noted that Victoria Police revoked all warrants that were not executed.

A warrant may not be executed for a number of reasons. Generally, this is due to the operation concluding before there was an opportunity to install a surveillance device.

Findings: warrants

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

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

Specifically, we found the following requirements were met:

- the applicant was a law enforcement officer
- approval was provided by an authorised police officer
- the applicant's name and the nature and duration of the warrant were specified including the kind of device sought

[3] This number includes one warrant for which records were destroyed just outside the reporting period. In cases where a warrant was not executed, a signed and dated 'Reconciliation of Surveillance Device Material' form was inspected.

- a sworn affidavit was provided in support
- the PIM was notified of the application
- the application was made to a Supreme Court judge or magistrate, as appropriate.

In addition to meeting these requirements, Victoria Police made 2 applications to extend an existing warrant and one application to vary a warrant to remove a condition. These applications were made to the relevant judge as required by section 20 of the SD Act.

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

All surveillance device warrants issued to Victoria Police complied with section 18 of the SD Act by specifying the following:

- the name of the applicant and alleged offence
- the date the 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 the 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
- the name and signature of the issuing authority (magistrate or judge).

Victoria Police did not make an application for an assistance order, a retrieval warrant, or for an emergency authorisation to use a surveillance device during the reporting period.

For the inspected warrants, Victoria Police revoked a warrant on 19 occasions via written instrument signed by a delegate of the Chief Commissioner of Police, in accordance with section 20A of the SD Act. Victoria Police revoked warrants in cases where it decided the use of a surveillance device was no longer necessary for the purpose of enabling evidence to be obtained of the commission of the offence or the identity or location of the offender.

Victoria Police's close monitoring of whether the grounds to keep each warrant active still exist is evidenced by the high rate of revocations (61%). For each revoked warrant where a surveillance device was installed, Victoria Police first discontinued the use of the device pursuant to section 20B of the SD Act.

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 notice given under section 20A(3) for the revocation of a warrant

- each emergency authorisation, and the 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
- a copy of each evidentiary certificate issued under section 36 of the SD Act.

Victoria Police complied with these requirements for the inspected records.

Did Victoria Police keep all other necessary records?

Victoria Police must also 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
- the destruction of records or reports obtained by the use of surveillance devices.

We found that Victoria Police complied with these requirements.

Victoria Police kept details on the destruction of records and reports related to 19 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?

We found that Victoria Police kept an accurate register of warrants, as required by section 30O of the SD Act.

The register specified for each warrant file inspected the following particulars:

- the date the warrant was issued
- the name of magistrate or judge who issued the warrant, and 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
- any variation or extension of the warrant.

As Victoria Police did not exercise its emergency authorisation powers during the reporting period, there were no matters to be specified in the register in relation to section 30O(3) of the SD Act.

Findings: reports

Were reports to the magistrate or judge properly made?

Under section 30K of the SD Act, Victoria Police must within the time specified in the warrant make a report to the magistrate or judge who issued the warrant.

With respect to a surveillance device warrant, the report 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 the 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
- if the warrant was revoked by the chief officer under section 20A(2), the reason the device was no longer required and whether the PIM was notified of the revocation.

All reports made by Victoria Police under section 30K of the SD Act for warrants that ceased between 1 July and 31 December 2023 complied with these requirements and was made within the requisite timeframe.

Findings: transparency and cooperation

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

Following our inspection of records at Victoria Police's SPU, we suggested that for reporting the use made of information obtained by a device, the utility of the report made under section 30K of the SD Act would be further improved by apprising the issuing authority of the number of accused persons to whom the use relates. Victoria Police's SPU agreed to amend its report template to ensure it specifies the number of accused persons interviewed during which time information obtained by the use of a device was communicated.

Did Victoria Police self-disclose compliance issues?

Victoria Police did not make any self-disclosures at the inspections conducted during the period.

Were issues identified at previous inspections addressed?

There were no historical issues to be addressed on this occasion as the issues identified from our previous inspection of Victoria Police surveillance device records were completed in our last inspection period.