



Surveillance Devices Inspection Report

Report by Integrity Oversight Victoria on its inspections of
surveillance device records during the period 1 July 2023 to
31 December 2023

Integrity Oversight Victoria

Level 8, 565 Bourke Street
Melbourne VIC 3000

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

Acknowledgement

Integrity Oversight Victoria acknowledges the Traditional Custodians of the lands on which we work and pays respect to Elders past, present and emerging. We recognise and celebrate the diversity of Aboriginal peoples and their ongoing cultures and connections to the lands and waters of Victoria.

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

© Integrity Oversight Victoria 2025



You are free to reuse this work under a Creative Commons Attribution 4.0 Licence provided you credit Integrity Oversight Victoria as author, indicate if changes were made and comply with the other licence terms. The licence does not apply to any third-party material, images or branding including government logos.

Copyright enquiries may be directed to communications@integrityoversight.vic.gov.au.

ISSN 2982-2912 (online)
Published May 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	4
Introduction.....	6
Our role	6
How we assess compliance	6
How we report on compliance	6
Department of Energy Environment and Climate Action.....	7
Environment Protection Authority	8
Game Management Authority	9
Independent Broad-based Anti-corruption Commission.....	10
Findings: warrants	10
Findings: records.....	12
Findings: reports	14
Findings: transparency and cooperation.....	14
Office of the Special Investigator	16
Victorian Fisheries Authority.....	17
Victoria Police.....	18
Findings: warrants	18
Findings: records.....	20
Findings: reports	21
Findings: transparency and cooperation.....	22

Overview

This report presents the results of inspections conducted by Integrity Oversight Victoria¹ from 1 July to 31 December 2023 for records belonging to 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 January to 30 June 2023 period – the ‘reporting period’.

We inspected 100% of the records available for inspection.

The following 7 agencies 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)
- Office of the Special Investigator (OSI)²
- Victorian Fisheries Authority (VFA)
- Victoria Police.

IBAC and Victoria Police were the only agencies that exercised their powers under the *Surveillance Devices Act 1999* (Vic) (the SD Act) during this period.

This report identifies some compliance errors as a result of our regular inspections of surveillance device records during the 1 July to 31 December 2023 period. In the case of a finding that IBAC did not comply with a condition on how it was permitted to use a surveillance device [refer to pages 11 and 12 of this report for details], we found this sufficiently serious to make 2 formal recommendations to IBAC for remedial action.

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 (and during the reporting period, the OSI could), 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, and it ensures independent oversight of agencies’ compliance with the SD Act. We are required to inspect, from time to time, the records of each

¹ Until 10 February 2025, Integrity Oversight Victoria was known as the Victorian Inspectorate. This change was a result of the *Justice Legislation Amendment (Integrity, Defamation and Other Matters) Act 2024* that passed on 10 September 2024.

² The OSI was abolished on 2 February 2024 following the repealing of the *Special Investigator Act 2021*. We were advised by the Special Investigator that all OSI investigative and analytical functions ceased on 27 June 2023.

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). The inspections conducted at these 6-monthly intervals 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.

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. 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 being properly 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, as well as the action they take in response to any issues we raise.

In this report, we also assess compliance with the reporting requirements of section 30L of the SD Act. Each agency able to make applications to use a surveillance device is required to make an annual report to the Attorney-General that is also tabled in Parliament. We assess these reports against various criteria, including the requirement they be submitted to the Attorney-General by 30 September each year.

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 might 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 July to 31 December 2023. Inspection results are separately reported for each Victorian law enforcement agency with the authority to exercise powers under the SD Act.

Department of Energy Environment and Climate Action

DEECA's surveillance device warrants are administered by its Strategic Operations and Intelligence Unit.³

There were no ceased warrants or other surveillance device records at DEECA for the reporting period and as a result we did not conduct an inspection of DEECA records on this occasion.

In this report, our assessment of DEECA's extent of compliance is limited to whether the reporting requirements of section 30L of the SD Act were met. We found that DEECA's report for the 2022–23 financial year met all reporting criteria and was submitted to the Attorney-General by 30 September 2023.

³ Until 15 December 2024, this unit within DEECA was known as the Major Operations and Intelligence Unit.

Environment Protection Authority

The EPA has not yet made an application under the SD Act. Therefore, we did not conduct an inspection of records at the EPA.

We confirm however that the EPA made an annual report for the 2022–23 financial year under section 30L of the SD Act that met all reporting criteria and was submitted to the Attorney-General by 30 September 2023.

Game Management Authority

The GMA has yet to make an application under the SD Act, and as a result we did not conduct an inspection of records at the GMA.

We found the GMA made an annual report for the 2022–23 financial year under section 30L of the SD Act that met all reporting criteria and was submitted to the Attorney-General by 30 September 2023.

Independent Broad-based Anti-corruption Commission

IBAC's Internal Compliance team administers surveillance device warrants issued to IBAC. On 2 November 2023, we conducted an inspection of the 7 surveillance device warrants issued to IBAC. For one of these warrants, we identified a serious issue with how IBAC complied with a warrant condition and for which we have made 2 recommendations.

We also inspected records connected to the extension of each warrant, one variation application as well as an assistance order. These represented all eligible surveillance device records for the 6-month period ending 30 June 2023.

Findings: warrants

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

We found that all applications 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 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.

In addition to meeting these requirements, IBAC made 7 applications to extend an existing warrant, and one other application to vary a warrant. On each occasion, the application was made to the relevant judge as required by section 20 of the SD Act.

IBAC also made one application for an assistance order that complied with the requirements under section 21 of the SD Act – being in the same manner as an application for a warrant specified above.

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).

While all warrants issued to IBAC during the reporting period were in the proper form, we found that IBAC failed to comply with a condition on how it was permitted to use a surveillance device:

Finding: non-compliance with warrant condition on use of a surveillance device

A warrant that authorised the use of a listening device was issued by the Supreme Court of Victoria subject to the following condition:

That recording capabilities only be activated at times when intelligence or other observations indicate that:

[person of interest (POI) 1 and POI 2] are meeting at the premises; and [POI 1] is meeting with other persons of interest to the investigation at the premises.

The records we inspected showed that 2 listening devices were installed, and commenced recording shortly after the warrant was issued. Given the specific nature of the condition on the warrant, we queried IBAC on how it complied with this condition.

In our post inspection enquiries, IBAC stated that conversations captured by the devices were only reviewed if there was deemed to be an additional person at the premises. While these actions dealt with how audio recordings were reviewed, the condition on the warrant was concerned with the *activation* of recording capabilities rather than the monitoring of those recordings.

Over a 6-day period from when they were installed, rather than recording conversations that related to meetings between persons of interest, these devices recorded all conversations. This was because the listening devices were programmed to record on voice activation.

From our enquiries with IBAC into the extent to which privacy was impacted during this period, IBAC confirmed that the surveillance device captured conversations of persons in contravention of the condition on the warrant.

IBAC's response to this finding:

IBAC has informed us that it acknowledges our finding of non-compliance with the warrant condition and accepts the two recommendations referred to below in full. In this regard, we look forward to inspecting IBAC's updated templates and procedure as well as the supplementary report under section 30K of the SD Act when these records are available.

Recommendation 1

To mitigate against the future risk of not complying with a condition imposed on a warrant, we recommend that IBAC's Technical Surveillance team keep detailed records to show how the installation and/or use of a device has complied with any conditions specified on the warrant. In this case, IBAC's records simply stated that they had 'managed recording as per conditions on the warrant'. This was incorrect.

In addition to supporting IBAC's quality assurance processes, this change will make the report to the judge or magistrate who issued the warrant more informative, and by extension, provide greater transparency on compliance with a condition to the issuing authority. In this respect, we note that section 30K(2)(b)(ix) of the SD Act requires each report to 'give details of the compliance with the conditions (if any) to which the warrant was subject'.

IBAC's response to recommendation 1:

IBAC commits to implementing these improvements in a timely manner [and has undertaken to update the following templates and procedure]:

- *IBAC's covert memo template [to give additional guidance] to ensure Technical Surveillance Unit staff keep detailed records adequate to demonstrate compliance with any condition*
- *IBAC's section 30K report template [to include reminders and guidance] to ensure section 30K reports provide an accurate statement to the issuing judge of the compliance with [any] conditions*
- *the Compliance team's internal surveillance device procedure to provide detailed guidance on compiling a section 30K report where the warrant was subject to a condition*
- *the template email which is sent out at the time of issue of warrant to place increased importance on compliance with conditions of a warrant and to ensure Technical Surveillance Unit staff and Investigations staff are aware of their obligations in relation to record keeping and reporting in such circumstances.*

Recommendation 2

As a result of this finding, the report IBAC made under section 30K of the SD Act incorrectly reported that IBAC complied with the conditions to which the warrant was subject. We recommend that IBAC make a supplementary report under this section so that the judge who issued the warrant is apprised that listening devices were activated in a manner that contravened the warrant condition over a 6-day period.

IBAC's response to recommendation 2:

IBAC will submit a supplementary section 30K report [...] as soon as practicable.

There were no applications relating to a retrieval warrant or for an emergency authorisation to use a surveillance device during the reporting period. For the inspected warrants, IBAC did not revoke a warrant via a written instrument signed by a delegate of the IBAC Commissioner.

In the case of an assistance order, we previously reported that IBAC disclosed an error with the form of this assistance order issued by the Supreme Court – specifically, that it was not endorsed on the relevant warrant under section 22(4) 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 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 with respect to the 7 warrants 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 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 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, noting no records or reports were destroyed during the reporting period. At the inspection, IBAC informed us that it had recommenced undertaking the destruction of relevant records and reports under section 30H(1)(b) of the SD Act. Records related to these destructions will form part of the records made available at the next inspection.

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 each inspected surveillance device warrant:

- the date the warrant was issued
- the name of the 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
- 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.

While the reports made by IBAC for the 7 inspected warrants were made within the requisite timeframe, IBAC disclosed at inspection that one report omitted a further use of information obtained by a device installed under the warrant. We confirmed at the inspection that IBAC corrected the error in a supplementary report given to the issuing judge. Additionally, we have recommended that IBAC make a supplementary report to correct information reported under section 30K of the SD Act. See Recommendation 2 above.

Was the annual report to the minister properly made?

We assessed IBAC's compliance with the reporting requirements of section 30L of the SD Act and found that the annual report made by the Commissioner for the 2022-23 financial year met all reporting criteria and was submitted to the Attorney-General by 30 September 2023.

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 in the case of 3 warrants, all surveillance devices were retrieved at least 2 weeks before each warrant expired. While the SD Act does not give a timeframe for revoking a warrant, unlike for the discontinuance of use of a device, we

suggested to IBAC that it is better practice for a warrant to be revoked as soon as practicable once it has decided the use of the authorised device(s) is no longer required.

IBAC agreed to bring this better practice requirement to the attention of investigators. In support of this change, we suggested that IBAC consider bringing this requirement to the attention of investigators via emails used to notify them of newly issued warrants. We subsequently confirmed at the next inspection that IBAC had revised its warrant notification email template to include this additional information.

Did IBAC self-disclose compliance issues?

IBAC disclosed during the inspection that for a warrant from the previous reporting period, the applicant recorded an entry in the use and communication register that was backdated to precede when the section 30K report was made to the issuing judge as well as prior to our earlier inspection of the file. This use of information obtained by surveillance devices installed under the warrant was added to a supplementary report to the relevant judge that also included other previously omitted uses of information.

Were issues identified at previous inspections addressed?

We previously reported that IBAC made a supplementary report under section 30K of the SD Act to include additional uses made of information obtained by the surveillance devices installed under the warrant. This supplementary report was inspected by us at the November 2023 inspection.

Office of the Special Investigator

The SD Act was amended on 1 December 2021 to include the OSI as a relevant law enforcement agency. As previously noted, the OSI's investigative and analytical functions ceased during the reporting period. There were no relevant records to inspect at the OSI for this period.

We nonetheless confirm that the OSI made a report for the 2022–23 financial year that was compliant with the reporting requirements of section 30L of the SD Act.

Victorian Fisheries Authority

The VFA did not have any relevant records associated with warrants that ceased in the 6-month period ending 30 June 2023.

However, at an inspection conducted on 19 September 2023, we reviewed and provided feedback on finalised VFA procedures for administering surveillance device warrants. We confirmed the finalised procedures incorporated feedback we provided at the previous inspection with just one exception. In our post-inspection enquiries, the VFA agreed to make the additional update. We have since confirmed this change has been made.

At this inspection, we also reviewed the destructions register kept by the VFA. Since 2014, the VFA has only accessed surveillance device data online directly from Victoria Police, and therefore it does not keep records or reports obtained by the use of a device. The register shows the only records held by the VFA for the surveillance device warrants it has been issued with are those connected to briefs of evidence. All other records obtained by the use of a surveillance device are destroyed by Victoria Police following confirmation from the VFA that these are no longer required.

Additionally, we assessed the VFA's compliance with the reporting requirements of section 30L of the SD Act. We found the annual report made by the CEO for the 2022–23 financial year met all reporting criteria and was submitted to the Attorney-General by 30 September 2023.

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. We inspected all available TSU records for surveillance warrants that ceased during calendar 2023 on 4 June 2024.

We inspected all 42 surveillance device files administered by Victoria Police's SPU and TPU. This includes 40 issued warrants, and 2 warrants that were extended. In addition to records on the destruction of 27⁴ surveillance device warrants, we also inspected 18 evidentiary certificates and 2 assistance orders. Altogether, these represent all relevant surveillance device records for the reporting period.

Six surveillance device files at the TPU were inspected on 19 October and 16 November 2023, and 36⁵ files at the SPU were inspected from 13–15 November 2023.

In addition to finding some minor administrative errors with the information kept in its use and communication registers, we also identified an error with the information reported to the relevant judge for 2 warrants.

For the total number of warrants granted to Victoria Police for the period, 5 were not executed – representing 12.5% 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.

⁴ This number excludes 2 warrants Victoria Police's SPU included in its destructions checklist for the reporting period but for which no destruction records were compiled. The SPU informed us that it no longer makes these records for warrants that were not executed. We support this process change since the SD Act is concerned with the destruction of records or reports obtained by the use of a surveillance device.

⁵ This includes one file connected to a warrant under which a device was installed during the reporting period, however the warrant ceased outside this period because it was extended.

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 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.

In addition to meeting these requirements, Victoria Police made 2 applications to extend an existing warrant. On both occasions, the application was 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).

In the 2 instances Victoria Police was issued with an assistance order under section 22 of the SD Act, the order was endorsed on the relevant warrant and specified all the required matters.

Victoria Police did not make an application for 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 28 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 (72%).⁶ For each revoked warrant where a surveillance device had been installed, Victoria Police first discontinued the use of the device pursuant to section 20B of the SD Act.

⁶ This percentage considers a total 39 surveillance device warrants were ceased during the reporting 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 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 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
- the destruction of records or reports obtained by the use of surveillance devices.

We found that Victoria Police complied with these requirements, except in the case of 2 warrants where the respective use and communication register omitted a use of information obtained by the device(s) that was given in the report made under section 30K of the SD Act for each warrant. In both cases, Victoria Police's TPU confirmed the reports were correct. We subsequently confirmed that these registers were amended to show the additional uses of information obtained by the use of the surveillance devices.

Victoria Police kept details on the destruction of records and reports related to 27 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, 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
- any variation or extension of the warrant.

Since 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 is required within the time specified in the warrant to 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 January and 30 June 2023 were made within the requisite timeframe, however 2 reports were found to contain an error.

Finding: information omitted from the report given to the judge

Victoria Police is required to report to the judge who issued the warrant, among other things, the general use of information obtained by use of a surveillance device. For one warrant, we found a use recorded in the use and communication register was not given in the report to the judge for the same warrant. Enquiries with Victoria Police's TPU confirmed that the report omitted this use. We subsequently inspected a supplementary report under section 30K of the SD Act that corrected this omission.

In cases where a warrant is revoked under section 20A(2) of the SD Act, the report to the issuing judge must state whether the PIM was notified of the warrant's revocation. For one such revoked warrant, we found that the report made by Victoria Police's TPU did not include this information. We later inspected an amended report that was submitted to the relevant judge.

Was the annual report to the minister properly made?

We found that Victoria Police complied with the reporting requirements of s 30L of the SD Act. The annual report made by the Chief Commissioner for the 2022–23 financial year met all reporting criteria and was submitted to the Attorney-General by 30 September 2023.

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.

From our inspection of destructions-related records at Victoria Police's SPU, we observed that a form used for confirming the destruction of surveillance device material was changed to remove a specific declaration. In our post-inspection enquiries, we requested a copy of any related procedural documents. Victoria Police's SPU subsequently provided us with a copy of new instructions it uses to confirm the destruction of records or reports. We found these instructions support Victoria Police's destruction obligations under section 30H(1)(b) of the SD Act.

In response to a warrant that was allowed to expire 10 days after it was no longer required,⁷ we suggested to Victoria Police's TPU that it would be better practice to cause a warrant to be revoked as soon as practicable once satisfied the warrant is no longer required – in cases where at least 2 business days of validity remain. Although the SD Act does not give a timeframe for a delegate of the Chief Commissioner of Police to revoke a warrant once satisfied the use of any authorised devices are no longer required, during our post-inspection discussions, Victoria Police's TPU agreed to implement this process change.

Integrity Oversight Victoria has previously reported that we are engaged in discussions with Victoria Police on its use of a particular type of surveillance device. Although our enquiries in

⁷ The continued use of a surveillance device installed under this warrant came under the authority of a new warrant, therefore making the original warrant obsolete.

this matter remain ongoing, these discussions have progressed, and we may provide an update in the next inspection report.

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 no issues were identified during our inspection of Victoria Police surveillance device records in the previous inspection period.