



The permanent installation of listening devices in prisons and their use by Victoria Police

An Integrity Oversight Victoria inspection report examining warrants authorising Victoria Police to use listening devices in prisons between 2008 and 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, November 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.

Published November 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	1
Our recommendations.....	4
<i>Surveillance Devices Act 1999</i> and our role.....	6
Background	7
Inspection findings	10
Findings 1-3: transparency in warrant applications.....	11
Findings 4-6: privacy in warrant applications	16
Findings 7-8: transparency in Victoria Police records.....	21
Finding 9: Victoria Police records on management of privacy	26
Finding 10: Victoria Police procedures	28
Findings 11-12: oversight engagement – transparency	29
Victoria Police’s position	33
Glossary.....	34

Overview

1. In 2023, in response to questions by Integrity Oversight Victoria¹, Victoria Police revealed it had permanently installed listening devices and equipment for use in some Victorian prisons. These devices were installed without the authority of a warrant issued under the *Surveillance Devices Act 1999* (SD Act).²
2. The permanent installation of at least 115 listening devices occurred at various junctures between 2000 and 2018.³ Many of these installations occurred when the prison was undergoing construction or renovation.
3. In this report we describe the listening devices and equipment used to facilitate their use, which were permanently installed in prisons as ‘integrated listening devices’.
4. While integrated listening devices were in place from at least 2000, Victoria Police was unable to show any guidance that supported this methodology from its outset. The earliest supporting information Victoria Police provided was from 2018.
5. After 2 years of extensive engagement through meetings and correspondence with Victoria Police to understand what listening devices and related equipment were in prisons and the extent of information supporting their instalment, we notified them in May 2025 that we would conduct an irregular⁴ inspection of their use of surveillance devices in prisons. Our engagement with Victoria Police included discussions with its Technical Surveillance Unit (TSU) (the unit responsible for installing and managing surveillance devices) to understand how the integrated listening devices are installed and work.
6. This report addresses the use of such devices for the period 2008 to 2024.⁵
7. We reviewed 99 warrants relating to the use of listening devices in a prison and assessed:
 - whether Victoria Police was transparent with judges and the Public Interest Monitor (PIM) about the integrated listening devices when it applied for warrants
 - whether Victoria Police was clear it was not seeking to install any devices but intended to activate integrated listening devices

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* and the change to our name was proclaimed on 26 November 2024.

² The regulation against using a surveillance device to overhear, record, monitor or listen to a private conversation to which the person is not a party, without the express or implied consent of each party to the conversation, does not apply where the installation, use or maintenance of a listening device is in accordance with a warrant.

³ Victoria Police indicated that some of these devices are inactive or degraded and therefore cannot verify whether they are still functional.

⁴ Additional to our regular biannual inspections conducted for the purpose of making 6-monthly reports to Parliament under section 30Q(1) of the SD Act.

⁵ We selected this period as our own records (which include records of the Office of the Special Investigations Monitor (SIM) which operated from 2004-2013) dated back to 2008. This enabled us to independently structure an inspection without requesting further information from Victoria Police.

- whether the records provided to us, and previous inspecting bodies, provided accurate information.
8. We did not identify any warrant applications where Victoria Police disclosed the integrated listening devices to the judge or the PIM. Most applications were for the ‘installation and use’ of listening devices, although in most cases no installation was necessary.
 9. We also identified that records made available at previous inspections referred to the installation of listening devices under warrant, which we now know inaccurately reflected Victoria Police’s use of integrated listening devices. For warrants issued between 2008 and 2024, the records predominately stated that listening devices were ‘installed’ and ‘retrieved’. However, from our inspection of additional internal Victoria Police records, we now understand in most cases no installation or retrieval of a device occurred, and instead the integrated listening devices were activated or deactivated. This at least coincided with the issue of the warrant.
 10. It is apparent the covert use of listening devices in prisons is a significant investigative tool and one that Victoria Police is eager to keep confidential to protect its efficacy. This is why Victoria Police indicated it does not typically discuss confidential methodology in applications for surveillance device warrants.⁶ However, the methodology should be disclosed to judges and the PIM.
 11. It is our understanding that, while the integration of the listening devices occurred without proper authority, Victoria Police’s process was that it only used these devices under the authority of a surveillance device warrant. This was in part backed by our findings, as we did not identify any unauthorised use of listening devices. However, we could not definitively confirm that listening devices were activated only in accordance with a warrant as Victoria Police was unable to show contemporaneous records, such as logs, to confirm when the listening devices were activated.
 12. We also understand that maintenance was performed on these devices without the required authority of a warrant.
 13. Our role is to determine the extent of compliance with the SD Act by Victoria Police and its officers, and to table a report in Parliament on the results of our inspections. This enables transparency and accountability in cases where an agency has not met its compliance obligations under the SD Act.
 14. It is our assessment that Victoria Police did not comply with the SD Act when installing and maintaining integrated listening devices. That this issue occurred over a long period compounds the significance of the non-compliance. A reliance on the integrated listening devices risks impacting the permitted uses under the authority of warrants by virtue of the unauthorised original installation or later unauthorised maintenance.

⁶ We also attributed this to the siloed nature of information sharing within Victoria Police, whereby the unit responsible for drafting affidavits in support of warrant applications was not consistently aware of Victoria Police’s methodology for using listening devices in prisons.

15. We recognise that investigation of serious crimes is a legitimate aim for the use of surveillance devices in prisons; and for their use to be effective, it needs to be done covertly.
16. We carefully considered this factor, and our obligations under the SD Act, in producing this report. We sought to achieve a balance between transparency and accountability, and a reasonable protection of surveillance device methodologies through the level of detail we provide. The report highlights facts only to the extent they are crucial to supporting our findings and recommendations. Otherwise, we limit revealing information connected to this covert capability.
17. The use of surveillance devices is an intrusion on a person's right to privacy. It is necessary for the Parliament, and by extension, the public, to have assurance that surveillance devices are used in Victorian prisons in compliance with the SD Act. In cases where a prosecution relies on information obtained from these listening devices, it is important that information relating to their installation and use be appropriately disclosed. Victoria Police is undertaking considerable work to determine the use of information collected from these devices so it can carry out a disclosure process.
18. Our recommendations, of which there are 8, are framed in this context. Victoria Police accepted all recommendations contained in this report – noting its acceptance of recommendation 8 was subject to a revision since made by us.
19. For procedural fairness, Victoria Police was given an opportunity to comment on this report. We incorporated these comments into the report, or made changes, as appropriate. Other comments made by Victoria Police about this report are included in the section titled 'Victoria Police's Position', on page 33.
20. Victoria Police emphasised to us that it has always acted in good faith and in accordance with the guidance it received. We note that Victoria Police immediately terminated its use of the integrated listening devices after becoming aware their use may be inappropriate. Further, we are aware it is now taking steps to remedy the situation, including removing certain equipment from prisons.
21. Victoria Police informed us that it considers the SD Act is not fit for purpose and it is seeking legislative reform to retrospectively permit the integrated listening devices. Although the SD Act may not entirely support modern surveillance needs, it is worth reflecting that Victoria Police has used integrated listening devices in prisons since the SD Act commenced.
22. This report does not address how it came to be that listening devices were integrated into Victorian prisons. This will be addressed in our second inspection which will also review warrants between 2000 and 2007.⁷ We will also consider what effect a 2012 Victorian Ombudsman report⁸ may have had on Victoria Police's practices, noting that a section of

⁷ During the inspection we identified there were approximately 80 warrants issued between 2000 and the end of 2007, marking a period of intensive use of this methodology. We did not consider warrants prior to 2000, as this falls under the now repealed *Listening Devices Act 1969*, under which we have no role.

⁸ The death of Mr Carl Williams at HM Barwon Prison – investigation into Corrections Victoria – April 2012 (G E Brouwer, Victorian Ombudsman) <https://www7.austlii.edu.au/au/other/VicOmbPRp/2012/8.pdf>

that report was devoted to the discovery of listening devices installed in Barwon Prison, potentially in breach of the *Listening Devices Act 1969*⁹ and the SD Act.

23. While agencies in other jurisdictions can be issued with a surveillance device warrant that can be exercised within Victoria (the execution of which may involve assistance from Victoria Police), these warrants are outside our remit and therefore a matter for relevant State and Commonwealth inspecting bodies to consider. They may also wish to examine the use of surveillance devices in prisons within their jurisdictions, if they have not already.

Our recommendations

Recommendation 1 To address the lack of transparency with judges who issued these warrants, we recommend Victoria Police disclose to the Chief Justice of the Supreme Court of Victoria that the affidavits made in support of 88 warrants omitted reference to the existence of, and the intention to use, listening devices previously installed without the authority of a warrant. We note that Victoria Police has already made such a disclosure to the PIM. We consider a further disclosure of this nature would assist in appropriately bringing this matter to the Court's attention.	Accepted
Recommendation 2 2.1 To achieve a better balance between transparency and protection of operational methodology, we recommend where it intends to use surveillance devices that do not rely on traditional installation methods (i.e. the use of novel capabilities), Victoria Police explore means to more transparently describe its methodologies with the judge or magistrate and the PIM when it makes surveillance device applications. This should provide the judge or magistrate and PIM with a clear understanding of the proposed use of surveillance devices (including the privacy impacts), whilst balancing a reasonable protection of methodology. This includes how the installation or activation of a surveillance device is described where a warrant is extended. 2.2 As part of this, Victoria Police should consider the level of information sharing between the TSU, investigators and the Affidavit Preparation Section (APS) so they are apprised of appropriate details relevant to making an application for a surveillance device warrant, or its extension. Victoria Police should report to IOV by 30 January 2026 on its proposal.	Accepted

⁹ The *Listening Devices Act 1969* was the predecessor to the SD Act. It dealt only with listening devices while its replacement, the SD Act, deals with a broader range of surveillance devices.

Recommendation 3 Victoria Police, in consultation with the PIM, to develop standardised wording in its applications for surveillance devices on the steps it will take with respect to legal professional privilege (particularly where there is a risk of such privileged discussions being captured).	Accepted
Recommendation 4 Victoria Police to revise its process for recording the specific activities undertaken to install, activate, maintain, deactivate and retrieve a surveillance device. Its records and processes should aim to provide a high level of confidence to inspections/oversight bodies on the actual activities undertaken in executing the surveillance device warrant. These records should also aim to provide reliable and authoritative information for officers who are required to complete section 30K reports made to judges or magistrates. As part of this, training and guidance should be provided on the expected levels of detail and the sources which are to be relied upon in preparing these reports.	Accepted
Recommendation 5 To provide transparency to the judge or magistrate, and enable effective oversight of their use of surveillance devices, Victoria Police revise its process for section 30K reporting to be clear on the nature of any installation and activation of a surveillance device, and to accurately report on the date and time a device was activated where the use of the device is restricted (such as to coincide with the presence of the person under investigation). This approach should apply more broadly than solely on the use of surveillance devices in prisons: active consideration should be given to ensuring the section 30K reports provide an accurate picture of the use of surveillance devices under any warrant.	Accepted
Recommendation 6 Victoria Police to review its record-keeping process for surveillance devices so it keeps verifiable records that demonstrate the installation, activation, and deactivation of a surveillance device is consistent with the authority of a warrant. For prisons, Victoria Police should also keep records to correlate the presence of the target and other specified persons with the activation of surveillance devices. Victoria Police should report to IOV with a proposal that satisfies this recommendation by 30 January 2026.	Accepted

Recommendation 7 Victoria Police to revise its surveillance device policies and procedures to account for the specific processes recommended in this report.	Accepted
Recommendation 8 Where Victoria Police proposes or intends to use a new capability under the authority of the SD Act, that it proactively discloses this to IOV and considers providing any supporting legal advice. Where relevant, similar disclosure processes should occur for the Courts and the PIM.	Accepted

Surveillance Devices Act 1999 and our role

24. The SD Act commenced on 1 January 2000, replacing the *Listening Devices Act 1969*.

25. 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 can apply to the Supreme Court for a surveillance device warrant authorising use of the following types of devices:

- data
- listening
- optical
- tracking.¹⁰

26. The following law enforcement agencies can use surveillance device warrants under the SD Act:

- Victoria Police
- Independent Broad-based Anti-corruption Commission (IBAC)¹¹
- Department of Energy, Environment and Climate Action
- Victorian Fisheries Authority
- Game Management Authority
- Environment Protection Authority.

27. Since 2013, the PIM has tested the content and sufficiency of the information relied on and the circumstances of warrant applications made by law enforcement agencies, including

¹⁰ For use of a tracking device only, an application may be made to the Magistrates' Court.

¹¹ In addition to court issued warrants, senior officers of Victoria Police and the IBAC can, in certain emergency situations, authorise the use of surveillance devices.

applications for the use of surveillance devices. For this purpose, the PIM is entitled to make submissions to the Court regarding a warrant application.

28. 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 using such devices.
29. We provide independent oversight of agencies' compliance with the SD Act. We must periodically inspect the records of each agency and report on the results of our inspections at 6-monthly intervals to each House of Parliament and the responsible Minister (Attorney-General). The inspections conducted at these 6-monthly intervals constitute our regular inspection framework. Where we identify a significant compliance concern, we can undertake further inspections, as we have done for the issues outlined in this report.

Background

The Tasmanian Review

30. In a decision made on 28 July 2022, Justice Brett of the Supreme Court of Tasmania, ruled to exclude evidence obtained by using a surveillance device in a prison by Tasmania Police. His Honour considered that an application for a surveillance device warrant did not fully address the risk that a surveillance device might record private conversations unrelated to the investigation, such as conversations between legal representatives and their clients.¹²
31. This warrant was sought to enable Tasmania Police to install and use surveillance devices to record a meeting. Once that meeting took place, the surveillance devices were left to continuously record until they were retrieved 2 months later. This had the potential for all conversations in the relevant meeting room to be recorded over that 2-month period.
32. Because of this, in November 2022, the Tasmanian Government announced a review into the use of surveillance devices in Tasmanian prisons.¹³ The initiation of this review, which we became aware of in March 2023, prompted us to enquire with Victoria Police on its use of surveillance devices in prisons.
33. Nothing in this report suggests that a similar issue has occurred with Victoria Police as it did with respect to the Tasmania Police.

Engagement

34. We first wrote to Victoria Police in July 2023 to seek clarification on how, when using surveillance devices in prisons, it mitigated the risks of capturing private conversations unrelated to investigations. We also enquired about the steps it takes to safeguard privacy.

¹² *Tasmania v Thompson* (No 2) [2022] TASSC 55.

¹³ Later reported in *Report of the Review of the use of Surveillance Devices in Prisons Tasmania 2024*. Damian Bugg AM KC.

35. Between late 2023 and early 2024, we made further enquiries with Victoria Police to clarify information it gave about its use of surveillance devices in prisons, including whether any devices were permanently installed. Victoria Police disclosed that listening devices and equipment to facilitate their use were integrated into various prisons between 2000 and 2018. This was not done under the authority of a surveillance device warrant. Our analysis of information provided by Victoria Police indicates there were at least 115 individual integrated listening devices installed in this manner.
36. As the SD Act requires a warrant to covertly install and use a listening device, we enquired with Victoria Police about what guidance it had to support its use of integrated listening devices.¹⁴ Victoria Police advised it received information in 2018 that indicated its methodology complied with the SD Act, however it could not locate or identify any earlier information, including guidance received in this matter. This meant there does not appear to be any guidance supporting Victoria Police's practice for installing listening devices in prisons from 2000 to 2017. While the 2018 information indicated that Victoria Police's methodology complied with the SD Act, we raised questions about this for Victoria Police to consider.
37. As a result, subsequent information provided by Victoria Police indicated the practice of installing and using listening devices without a warrant was non-compliant with the SD Act. It also stated there were implications if information obtained from these devices was relied on in prosecutions.
38. As well as the unauthorised installation of the integrated listening devices, we also understand that maintenance was performed upon these devices over the years without the authority of a warrant.
39. Victoria Police subsequently commenced an assessment for decommissioning the integrated listening devices in prisons. This decommissioning process was initially intended to render these devices irreversibly unusable. We understand the decommission process is now focused on removing equipment to render the integrated listening devices inoperable until such time as a new warrant is issued to enable re-installation of this equipment. Victoria Police also indicated it intends to pursue retrospective legislative reform so the installation of the integrated listening devices would be compliant with the SD Act.
40. Lastly, we are also aware that Victoria Police is undertaking considerable analysis to identify the extent to which information from these devices was used, including in prosecutions, so that appropriate disclosures can be made.

Initiation of inspection

41. Because the use of integrated listening devices has spanned 25 years, we decided it was necessary to re-inspect every surveillance device warrant issued to Victoria Police over this period that related to a prison. Given the size of the inspection, and the likelihood of further questions arising from our inspection of the records, we divided it into a 2-phased inspection, with the first phase covered by this report.

¹⁴ See section 6 of the SD Act which permits the installation of listening devices in other limited circumstances – none of which apply to integrated listening devices.

42. On 9 May 2025, we notified Victoria Police that we would inspect their surveillance devices records connected to the installation of listening devices in Victorian prisons.¹⁵ Prior to notifying Victoria Police of the inspection, we undertook an internal assessment of records from the previous inspecting body for the SD Act, the Special Investigations Monitor, and our own archived inspection records. Altogether, these records cover the period since 2008. From this preliminary analysis, we identified all information relating to the use of surveillance devices in prisons between 2008 and 2024 and developed an inspection criteria and methodology.¹⁶
43. Through this process, we identified 99¹⁷ surveillance device warrants that appeared to authorise the use of surveillance devices in various prisons. We subsequently requested that Victoria Police make these warrants available for inspection, including records relating to the installation, use, and retrieval of the surveillance devices. We also requested registers and ledgers kept by Victoria Police which recorded all surveillance device warrants it obtained from 1 January 2000 to 25 May 2025. Records prior to 2008 were sought to understand the extent surveillance devices were used under warrant during the period to be covered by the planned second inspection phase.
44. Our second phase will explore questions relating to the origins for the installation of integrated listening devices and their continued use over an extended period. We will also assess the effect of the 2012 Victoria Ombudsman report on Victoria Police's practices and whether any opportunities were missed to re-evaluate their methodology to ensure compliance with the SD Act. This will be reported separately once completed.
45. The focus for our first inspection was **Transparency, Privacy and Procedures**.
46. This inspection sought to understand whether Victoria Police was transparent about the existence of integrated listening devices. It also considered whether Victoria Police took necessary steps to manage the privacy of persons whose private activities and conversations were monitored or recorded by a listening device in a prison.
47. Furthermore, the inspection sought to understand to what extent surveillance devices were used in prisons and whether Victoria Police had appropriate policies and procedures in place to manage their use.
48. Therefore, our inspection sought to answer the following four questions:

¹⁵ Under 30P(1) of the SD Act, we must, from time to time, inspect the records of a law enforcement agency to determine the extent of compliance with the SD Act by the agency and law enforcement officers of the agency.

¹⁶ For the first 6 years of its operation, there was no independent inspection framework in place in the SD Act. An oversight framework became operative on 1 July 2006, a role that was undertaken by the now defunct body, the Special Investigations Monitor and then assumed by the Victorian Inspectorate in 2013.

¹⁷ A further 2 warrants were identified by Victoria Police after the inspection notification. While this brought the total to 101, we later determined 1 of these additional warrants, and 1 warrant we had selected, did not relate to a prison.

Question 1: Was Victoria Police transparent with Judges, the PIM and oversight bodies regarding its use of surveillance devices in prisons under the SD Act?

Question 2: How was privacy dealt with?

Question 3: To what extent have surveillance devices installed without authority been used, or maintained, in prisons and how has the information obtained from these devices been used?

Question 4: Were appropriate policies, procedures and guidance in place?

Inspection findings

49. This report relates to one kind of surveillance device: listening devices.

50. The SD Act defines this as ‘*any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation*’.¹⁸

51. The threshold to apply for a surveillance device is where a Victoria Police officer, on reasonable grounds, suspects or believes that an offence has been, is about to be or is likely to be committed and the use of a surveillance device is or will be necessary for the purpose of an investigation into that offence or enabling evidence or information to be obtained of the commission of that offence or the identity or location of the offender.¹⁹

52. We inspected 99 warrants issued between 2008 and 2024 which related to a prison. Of these warrants, 88 related to the use of integrated listening devices. Many of the warrants we inspected concerned the investigation of serious offences, such as unsolved murders.

53. 82 warrants inspected were managed by the Special Projects Unit (SPU), the area of Victoria Police which administers most of the surveillance device warrants. 17 warrants were administered by Professional Standards Command (PSC) and its predecessor, the Ethical Standards Department (ESD).²⁰

54. Our inspection was structured so we first inspected:

- the 99 warrant files
- internal records related to making applications for warrants
- affidavits which accompanied each application
- the original warrants
- reports to the judges about how the warrants were used.

¹⁸ See section 3(1) of the SD Act.

¹⁹ Ibid s 15. To apply for a surveillance device, the Victoria Police officer must first have approval from a senior officer or authorised police officer.

²⁰ In most instances, the warrants at PSC/ESD appeared to be administered as part of an ‘overflow’ function, where it assisted the SPU to administer warrants when capacity permitted.

55. We then verified information from the above against detailed records kept at the TSU. This included information outside the scope of our regular 6-monthly inspections, and therefore, it was not previously assessed.

56. Our report covers a range of findings, which are detailed in individual sections shown below. For some findings, which we consider have important consequences or require process improvements, we make recommendations to Victoria Police. Each finding is detailed against the specific assessment that we conducted.

57. In total we make **8 recommendations**.

58. We also considered the use of information obtained from these devices. We found the information was used for various purposes, including for the prosecution of persons. Because Victoria Police is undertaking ongoing work in this area to determine the extent of use and to make appropriate disclosures, we did not undertake further assessments related to this during the inspection. We expect Victoria Police to report to us on the outcome of its assessment and disclosure activities once finalised.

Findings 1-3: transparency in warrant applications

Outline

59. This section details our findings after assessing Victoria Police's transparency with judges and the PIM when applying for surveillance device warrants to use a listening device in a prison. Our assessments were designed to understand if Victoria Police had openly disclosed that it intended to use integrated listening devices in the prisons, which we now know were installed without the authority of a warrant. We also sought to understand whether there were any differences between how it described the use of integrated and non-integrated listening devices in its applications.

60. We make 2 recommendations at the end of this section.

Finding 1

Assessment

If a warrant was sought for the use of a surveillance device in a prison with integrated listening devices:

- was the existence of this capability disclosed to the judge (and from 2013 onward, the PIM)?
- was the proposed installation or activation of surveillance devices described in the application?
- was this accurate?

Finding

We found no applications where Victoria Police indicated it intended to use integrated listening devices nor any that disclosed

their existence. We consider that judges and the PIM should have been apprised of this information.

The way surveillance devices were to be installed or activated was not addressed in the applications.

We attributed this to a siloing of information between key areas of Victoria Police and a mistaken belief that surveillance devices would be, or had been, installed and removed under the authority of each warrant.

We make **1 recommendation** that Victoria Police disclose these omissions to the Supreme Court, and **1 recommendation** focused on achieving a better balance between the protection of sensitive surveillance methodologies and meaningful transparency to those considering applications for warrants.

The recommendations are provided in full at the end of this section.

61. It is our understanding that if an investigator was seeking the use of a surveillance device in a prison, the application would only be endorsed by the TSU to proceed if there was a viable means to capture evidence in accordance with the warrant being sought. This would include whether integrated listening devices were available. In most cases, integrated listening devices were utilised. The existence of the integrated listening devices was therefore integral to enable applications for warrants to proceed.
62. Of the 99 prison-related warrants we inspected, 88 related to integrated listening devices. No affidavit made in support of an application for any of these 88 warrants revealed to the issuing judge that Victoria Police intended to use integrated listening devices or disclosed the existence of these devices.
63. Under the SD Act, a surveillance device warrant may authorise, among other things, the use of a surveillance device on specified premises, in or on a specified object, or in respect of the conversations and activities of a person. In all cases, a warrant authorises the installation, use and maintenance of the surveillance device.²¹
64. In 73 of these 88 warrants, the application sought authorisation for the ‘installation and use of’ surveillance devices, although there was no requirement to install a surveillance device on those occasions.²² The remaining 15 sought authorisation for the ‘use’ of surveillance devices.
65. While these warrants were granted based on the information presented in the affidavits, it is our view that Victoria Police should have disclosed the existence and proposed use of the integrated listening devices to each judge at the time of application. To do so would provide a level of transparency in the application commensurate with the degree to which

²¹ See sections 19(1) and 19(2) of the SD Act.

²² Of these, three warrants from late 2008 to early 2009 sought ‘continued installation and monitoring’ or ‘continued installation or use’ but this refers to the fact that there were earlier warrants for the same locations.

privacy is affected by using covert surveillance devices. It would also provide an opportunity for judges to consider the appropriateness of the use of listening devices previously installed without a warrant i.e., the integrated listening devices.

66. As there was no disclosure to the judges, it also appears there was no disclosure to the PIM which uses the same documents to test the content and sufficiency of each application.
67. While the scale of these omissions is of significant concern, it is noted that Victoria Police does not broadly discuss its covert methodologies internally nor in applications to the Court to protect its capabilities. Even within the TSU, information about the integrated listening devices capability was apparently known to only a limited group of officers.
68. This restricted information sharing within Victoria Police affected the preparation of affidavits for warrants, given those drafting the applications appeared to have no awareness of the integrated listening devices. The APS, which was responsible for preparing these affidavits, was not briefed about the existence of integrated listening devices. Consequently, they appeared to rely on a mistaken belief that surveillance devices would be, or had been, installed and removed under the authority of each warrant, when in fact integrated listening devices were to be used. This affected the ability of the investigators to respond accurately to questions the judges and PIM may raise concerning the installation and use of the listening devices.
69. This should have not occurred. Victoria Police's obligations to judges and the PIM when applying for surveillance device warrants should have achieved a better balancing of transparency over complete protection of methodology.
70. Importantly, beyond Victoria Police's obligations to be transparent with judges, there are full disclosure requirements within the SD Act. These require that an applicant must fully disclose to the PIM all matters of which the applicant is aware that are adverse to the application.²³ In this respect, the appropriateness of the use of integrated listening devices, which were installed without a warrant, should have at least been tested.
71. With a view to ensuring a better balance between transparency and the protection of methodologies, we make one recommendation to Victoria Police about how it describes methodology in its applications.
72. At Finding 5, we also discuss how the integrated listening devices were monitored by Victoria Police investigators. We consider that judges and the PIM should have also been informed of this process to have a clearer understanding of the privacy implications of how the listening devices could be activated by investigators and the extent to which safeguards were in place to ensure their use was strictly controlled.
73. We consider that Victoria Police should disclose this omission to the Supreme Court of Victoria. We understand that Victoria Police has already disclosed this issue to the PIM.

²³ See section 12C(1) of the SD Act.

Finding 2

Assessment

If the warrant was sought for a prison without integrated listening devices, how was the proposed installation or activation described in the application?

Finding

We found that Victoria Police's applications for these types of warrants did not typically describe the proposed installation.

This contributed to our general understanding of the expected level of information provided in affidavits for surveillance devices in prison. We make no adverse finding in this matter.

74. We assessed whether Victoria Police provided different information in applications for surveillance device warrants in prisons that did not rely on the integrated listening devices. We found there was no material difference between the level of detail provided. This was a result of Victoria Police's practice of not providing detail of its specific methodologies.
75. There were 6 warrants issued for prisons where the installation took place **after** warrant issue.
76. Other than on one occasion, there was no specific detail in the applications about how Victoria Police intended to install the surveillance devices. In these instances, the lack of detail did not present any issues, as the installation of listening devices accorded with the general practice of an actual physical installation following warrant issue.

Finding 3

Assessment

If a surveillance device warrant was extended:

- was the manner of installation or activation of devices under the original warrant disclosed to the judge and PIM in the application, as applicable?
- was this accurate?

Finding

We found that surveillance device warrant extensions did not disclose the manner of installation or activation of devices under the original warrant.

We found 12 warrants where incorrect information was provided.

In our view, restriction of information within Victoria Police was at least partially responsible for these errors, as was the reliance on

records which did not accurately describe the use of these surveillance devices.

The **2 recommendations** at the end of this section, made jointly with Finding 1, are intended to address this issue.

77. A surveillance device warrant can have a maximum validity period of 90 days. In cases where investigators require the use of a surveillance device beyond the period authorised in the warrant, an extension can be sought. An 'extension' follows the same process required to apply for the original warrant.²⁴
78. There is no express legislative obligation that requires an application to disclose how a surveillance device was installed under the original warrant; and our assessment is not whether Victoria Police did something that it was not required to do. Instead, our assessment focused on transparency and the accuracy of information presented to judges.
79. Under this assessment, we inspected 24 warrants which were extended or varied. No applications linked to these warrants specifically disclosed how the surveillance device was installed or activated under the original warrant (if one was installed). In most cases, the application referred to the previous warrant and what it authorised. We do not find this was problematic.
80. Of the 24, we identified 12 instances where the affidavit provided incorrect information regarding the installation of devices under the original warrant. Among these, the affidavits collectively made 41 references to the installation of surveillance devices under the originally issued warrants. However, this was inaccurate, as no installation occurred under the warrant due to the use of integrated listening devices.
81. Like our assessment at Finding 1, we consider this to be a direct result of the APS drafting affidavits without knowledge of the integrated listening devices and therefore being mistaken about how the listening devices were installed. It appears there was an assumption on their behalf that installation followed the usual practice of a device being physical installed after warrant; a view that was supported by other Victoria Police records that incorrectly referenced installations.

Recommendations

Recommendation 1

To address the lack of transparency with judges who issued these warrants, we recommend Victoria Police disclose to the Chief Justice of the Supreme Court of Victoria that the affidavits made in support of 88 warrants omitted reference to the existence of, and the intention to use, listening devices previously installed without the authority of a warrant.

²⁴ See sections 20(1) and 20(3) of the SD Act.

We note that Victoria Police has already made such a disclosure to the PIM. We consider a further disclosure of this nature would assist in appropriately bringing this matter to the Court's attention.

Victoria Police's response: accepted.

Recommendation 2

2.1 To achieve a better balance between transparency and protection of operational methodology, we recommend where it intends to use surveillance devices that do not rely on traditional installation methods (i.e. the use of novel capabilities), Victoria Police explore means to more transparently describe its methodologies with the judge or magistrate and the PIM when it makes surveillance device applications.

This should provide the judge or magistrate and PIM with a clear understanding of the proposed use of surveillance devices (including the privacy impacts), whilst balancing a reasonable protection of methodology. This includes how the installation or activation of a surveillance device is described where a warrant is extended.

2.2 As part of this, Victoria Police should consider the level of information sharing between the TSU, investigators and the APS so they are apprised of appropriate details relevant to making an application for a surveillance device warrant, or its extension.

Victoria Police should report to IOV by **30 January 2026** on its proposal.

Victoria Police's response: accepted.

Findings 4-6: privacy in warrant applications

Outline

82. This section details 3 findings we make about Victoria Police's approach to privacy in the applications for 99 surveillance device warrants we inspected. We assessed the applications to understand how the management of privacy was communicated to the judges.²⁵ We then determined whether the steps taken over the life of the warrant to manage privacy correlated with the information given in the application.

83. Privacy is a key element of the surveillance devices regime because the SD Act requires the judge to consider the extent to which the privacy of any person is likely to be affected.²⁶ The completeness and accuracy of information provided by Victoria Police then informs that decision.

²⁵ While a magistrate may issue a surveillance device warrant in some circumstances, only a Supreme Court judge may issue a warrant that authorises the use of a listening device.

²⁶ See section 17(2)(b) of the SD Act.

Finding 4

Assessment

Did Victoria Police indicate whether it intended to use surveillance devices in specific areas of the prison?

Finding

We found that Victoria Police was transparent regarding where it intended to use surveillance devices in prisons.

84. We did not identify any concerns with how Victoria Police indicated it would use surveillance devices or how it used them in practice. If Victoria Police indicated it would use a surveillance device in a particular location, the inspected records reflected it had only used it in this way.
85. However, for warrants that predated Victoria Police's use of the Interpose²⁷ system, there were limited records on the installation of the surveillance devices to enable us to definitively confirm when and how surveillance devices were installed and/or activated.

Finding 5

Assessment

Did Victoria Police describe in its applications how it would manage privacy when installing or activating a surveillance device in a prison?

Finding

While we identified that Victoria Police provided an adequate level of information in relation to privacy in its applications, it should have disclosed the process where investigators were able to independently activate listening devices and any safeguards relating to these activations.

Information on privacy in applications

86. We found there were differing levels of information about privacy provided in applications for surveillance device warrants. Prior to 2013, there was very limited detail regarding privacy in affidavits. Most applications from this period simply reflected that the privacy of the targeted person and certain other people would be affected (though in some cases, these did not acknowledge that the privacy of other persons would also be affected).²⁸

²⁷ A case management system used by Victoria Police to store and transmit law enforcement data.

²⁸ For 10 warrants the relevant affidavits provided no specific details regarding how privacy would be managed in specific areas of the prisons.

87. For later warrants, we noted that applications indicated that use of devices would be restricted to when the target was present.
88. It appears likely the inclusion of greater privacy-related information in affidavits from 2013 coincided with the introduction of the PIM and inter-agency discussions around expected levels of detail.
89. While the pre-2013 affidavits did not expressly explain the privacy related measures, these measures were nonetheless inherent as each affidavit sought the use of a surveillance device only at times when the targeted person was present.
90. For affidavits from 2013 onward, we identified more express consideration to addressing privacy. Many affidavits included a form of words as follows:

“Surveillance devices will not be activated in [the specified location] at the [Prison] unless [Person in prison] is present.

If a warrant is issued in this matter, the following steps will be taken to limit the extent to which privacy is affected: a) (...) only to the extent necessary to obtain evidence; b) (...) only be utilised and disseminated in accordance with the provisions of the (SD Act); (...) will be monitored by authorised Victoria Police staff members.’

(...) Any conversations recorded under warrant that are not relevant to the subject matter of the investigation or any other criminal offence will be identified and thereafter dealt with in accordance with the provisions of: a) the (SD Act); b) the Victoria Police Manual; c) any relevant Victoria Police policies and procedures.”

Other privacy related information

91. Applications from 2013 included a reasonable level of detail regarding privacy. However, we identified one process where certain information could have been included to provide insight into how Victoria Police monitored listening devices under warrant, and by extension, dealt with privacy.
92. This process involved the TSU activating a connection to the listening devices in a particular prison and setting up a monitoring suite for investigators to use the listening devices. Under this process, the investigators were instructed on how to activate the listening devices and how to switch the audio feed from one location to another. They then had access to the monitoring suite to independently use the listening devices as necessary.
93. In practice, this meant that investigators had precise control over the use of the listening devices and could activate them when they received information about the use of a particular part of the prison by the target of the investigation.
94. While this was an integral part of the process, we did not identify any procedures that governed how investigators activated the listening devices in this situation or safeguards to prevent inadvertent or unauthorised use. Victoria Police was unable to produce any records that showed when these listening devices were activated, nor any records that showed the activations correlated to the presence of the targeted persons.

95. Whilst we do not suggest that devices were activated when targeted persons were not present, there are clear risks attached to this process given there appeared to be no defined safeguards, controls or procedures that governed how it was used.
96. This process was not explained in applications for warrants, and it was not expressly detailed in records we previously inspected.
97. Information about this process could be relevant to considering privacy implications and the appropriateness of the processes to manage privacy impacts, including the recording of unrelated conversations.
98. While we do not make a recommendation, we find that this process should have been disclosed in applications and, at the least, should have been clearly captured in procedures. It is our understanding this process has recently changed so the TSU now directly manages the activation of listening devices, rather than investigators.
99. Separately, we also make a recommendation regarding the retention of additional records to enable us to determine when listening devices were activated and deactivated. This will allow us to make a definitive assessment as to whether the activation of the listening device corresponded with the terms of the warrant. See Finding 9 for more details.

Finding 6

Assessment

Did Victoria Police describe in its applications what actions it would take with respect to legal professional privilege, if discussions involving legal representatives may be captured?

Finding

We found inconsistent practices for detailing how legal professional privilege will be managed in warrant applications and made **1 recommendation** so that Victoria Police takes a consistent approach in future applications.

The recommendation is provided in full at the end of this section.

100. There is no legislative requirement within the SD Act that a conversation between a client and their legal practitioner not be overheard or recorded. However, where such conversations are not relevant to investigations, it is the usual practice of law enforcement agencies to outline the steps it will take to avoid capturing legally privileged discussions, or how it will deal with these if captured. At their discretion, judges may also apply conditions to warrants that prohibit the use of a surveillance device to record or overhear legally privileged discussions.
101. As part of the inspection, we assessed how the applications addressed the management of legal professional privilege and the extent to which conditions were applied to warrants.
102. For 61 warrants issued prior to November 2013, we found no affidavits identified how legal professional privilege would be managed. For this subset of warrants, 15 were issued with a

condition regarding legal professional privilege. After this time, there was a greater prevalence of conditions on warrants. However, the use of conditions and the wording in supporting affidavits was not always consistent, even in warrants after 2020.

103. Of the 38 warrants issued after November 2013, 9 included both a condition about legal professional privilege and a statement in the affidavit about how it would be managed. Three had only a condition about legal professional privilege, and 7 included only a statement on legal professional privilege in the affidavit. Legal professional privilege was not a factor in 10 of the warrants.
104. This finding does not imply that legal professional privilege was not considered, or that judges had not turned their mind to this matter, but rather Victoria Police should have a standardised process for how it deals with legal professional privilege in its surveillance device warrant applications.
105. We understand that Victoria Police is already considering this matter because of other reviews.²⁹

Recommendation

Recommendation 3

Victoria Police, in consultation with the PIM, to develop standardised wording in its applications for surveillance devices on the steps it will take with respect to legal professional privilege (particularly where there is a risk of such privileged discussions being captured).

Victoria Police's response: accepted.

106. We note that where a condition was stated on warrants, the reports to the issuing judge made under section 30K of the SD Act did not outline how Victoria Police had complied with the condition. In most instances, the report only stated that the condition was complied with.
107. As a matter of good administrative practice, and to ensure it is following a better practice approach, we suggest that Victoria Police provide specific detail in these reports on the steps it took to comply with conditions, such as, '*no legal professional privilege captured*' or '*captured on 5 instances and managed by quarantining*'.

²⁹ These reviews relate to The Tasmanian Review referred to on page 7 under 'Background', and the Royal Commission into the Management of Police Informants.

Findings 7-8: transparency in Victoria Police records

Outline

108. This section details our findings on the accuracy of Victoria Police's records regarding how it used surveillance devices under the warrants. We inspected a new set of records, provided by the TSU, to cross-reference and verify whether the records presented by Victoria Police were accurate and representative of the activities reported.

Finding 7

Assessment

What activities are recorded in the TSU's logs and ARS³⁰, and do they occur under the authority of a warrant (as applicable)?

Does each ARS accurately describe the circumstances of any installation or activation?

Finding

We did not identify any activities outside the authority of a warrant. However, we identified a related issue at Finding 9 regarding verifying the use of devices under these warrants.

We also found that records provided to us at prior inspections did not accurately reflect the installation and removal of surveillance devices, nor did they indicate the existence of integrated listening devices.

We consider this limited our ability to properly assess Victoria Police's compliance with the SD Act.

We make **1 recommendation** that Victoria Police revise its processes for recording the activities undertaken in relation to a surveillance device.

The recommendation is provided in full at the end of this section.

Activities

109. We did not identify any activities that occurred outside the authority of a warrant. However, this must be viewed in the context of Finding 9, where there were no contemporaneous records that allowed us to definitively assess whether surveillance devices were used within the parameters of the warrants.

³⁰ Action Report Sheet, a document made by the Technical Surveillance Unit that details the actions taken by its officers to execute the warrant, e.g. install, maintain or retrieve a surveillance device.

Assessment of ARS records

110. In our previous inspections, we relied on the ARS provided by Victoria Police's TSU. Whenever an action is taken under a warrant, for example to install a device, an ARS is prepared, or updated, to provide information on the warrant's execution such as where and when a surveillance device was installed, and who carried out the installation.
111. Our inspection of these records informs our assessment of whether Victoria Police has used surveillance devices in accordance with the warrants and made an accurate report to the issuing judge. These records are also used by other units of Victoria Police that manage warrants to prepare the reports to the relevant judge (or magistrate) about the use of the surveillance devices under the warrant.
112. During the inspection, we compared the ARS records against other records kept by the TSU, such as logs in the Interpose system about the use of the surveillance devices.
113. As Interpose was not used prior to 2010, for earlier warrants, we relied on handwritten ledgers which included details about warrants issued and the actions taken under them. We did not find these ledgers to be an authoritative resource as they used only generic terminology that did not reveal whether the integrated listening devices were relied on.
114. Despite this, our understanding now of which prisons had integrated listening devices, and the timeframe for when these were installed, allowed us to determine with reasonable confidence whether the integrated listening devices were relied on. This was confirmed by cross referencing our findings against Victoria Police's own assessments.
115. Through this comparison, we identified a range of inconsistencies in the ARS prepared by the TSU during the 2008 to 2024 period.
116. For integrated listening devices, the ARS records referred to the installation and retrieval of the device, and less frequently, when the device was activated and deactivated.³¹ In no instances did they indicate the use of integrated listening devices.
117. On a plain reading of these records, an inspections officer would have the impression that a listening device was installed and then removed – when in fact this had not occurred. It is important to recognise that the ARS were intended as the primary and authoritative source of how surveillance devices were installed, maintained or retrieved for the purpose of our inspections.
118. All previous compliance assessments relied on the accuracy of the information presented. A fundamental tenet of inspections is that information provided by the inspected agency be an accurate representation of the agency's activities.

³¹ It is important to understand that activation in this context mostly refers to the device being made available for use, not when it was switched on to record a conversation. The specific activation of the device to record was done remotely by investigators at the monitoring suites.

119. Inspections are not wide-ranging audits, but periodic assessments with some level of mutual trust. An inspection will only delve ‘behind the records’ when there is a trigger or inconsistency that prompts the need for further inspection.
120. Had the ARS indicated that integrated listening devices were being used, inspections officers would have had cause to look behind the records and seek further information about these surveillance devices. At the very least, confirmation could have been sought on whether these were authorised by warrant.
121. Information given in the ARS about the installation and retrieval of surveillance devices limited our ability to properly assess Victoria Police’s compliance with the SD Act and our understanding of the true level of compliance.
122. We note the ARS template only prompted actions connected to the ‘Installation’, ‘Maintenance’ and ‘Retrieval’ of a device. This may have led to a reliance on these terms to describe a variety of different activities. We further note that Victoria Police’s efforts to tightly limit knowledge of the integrated listening devices may have also been a contributing factor.
123. Given the centrality of these records to our oversight, Victoria Police should have actively considered whether the information it was presenting to inspecting bodies accurately represented the activities it undertook. It is likely our future inspections will need to rely on a greater range of primary source documents and look deeper into processes.

Recommendation

Recommendation 4

Victoria Police to revise its process for recording the specific activities undertaken to install, activate, maintain, deactivate and retrieve a surveillance device. Its records and processes should aim to provide a high level of confidence to inspections/oversight bodies on the actual activities undertaken in executing the surveillance device warrant.

These records should also aim to provide reliable and authoritative information for officers who are required to complete section 30K reports made to judges or magistrates.

As part of this, training and guidance should be provided on the expected levels of detail and the sources which are to be relied upon in preparing these reports.

Victoria Police’s response: accepted.

Finding 8

Assessment

Are Victoria Police’s section 30K reports to the judge who issued the warrant consistent with TSU records?

Do these accurately describe the circumstances of any installation or activation?

Finding

We found some inconsistencies between ARS records and section 30K reports to the issuing Judges.

While Victoria Police should have been more transparent in disclosing how it had used the surveillance devices, the information sources relied on, and its practice of protecting methodology, did not enable this.

We found 2 section 30K reports that indicated the use of permanent or 'fixed' listening devices. One of these appears to have been prompted by the judge who requested a supplementary report.

We do not consider these constituted a disclosure of the broader program of integrated listening devices and have assessed these further below.

We made **1 recommendation** regarding revisions to Victoria Police's section 30K report process.

The recommendation is provided in full at the end of this section.

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

125. 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 and 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.

126. For the 99 warrants we inspected, the section 30K reports consistently used the field 'Device location' to cover the reporting requirement about '*premises for installation of the device or the location for its use, as applicable*'. The data in this field typically only reflected the installation locations which were authorised by the warrant. This did not provide specific insight into what kind of installation took place, that is, whether it was a physical

installation or remote activation of an integrated listening device, or more specific information relating to where the devices were used.

127. While there is no requirement that Victoria Police make such a distinction in its reports, given the reports are intended as a transparency mechanism to the judge who issued the warrants, it would be better practice for Victoria Police to be transparent about any use of integrated listening devices.
128. Given the warrant applications did not indicate the use of integrated listening devices and referred to installations, it is possible that by lack of detail, the section 30K reports provided an impression that devices were in fact installed (when this may not have occurred).
129. As information in section 30K reports was often drawn from the ARS, and the investigators compiling the reports were not generally aware of the integrated listening device capability, Victoria Police's processes did not support the inclusion of detailed, nor always accurate, information in the section 30K reports. In this regard, we note Victoria Police's general practice of not disclosing details that would reveal sensitive operational methodology.
130. During the inspection, we also identified inconsistencies as to how Victoria Police reported 'the period the device was used'. Some section 30K reports reported it as the period from when the TSU made the surveillance device available for use to when it disabled access. Other section 30K reports however stated the period between which the device was specifically activated to record, or the exact dates on which the device was activated to record. In our view, the latter practice is preferable.

Permanently installed devices

131. We identified 2 instances where the report stated the device was permanently installed. Both warrants were independently managed by ESD/PSC.
- 2009 warrant:** a supplementary section 30K report to the judge for this warrant stated: *'Nil technical staff utilised as surveillance device is a fixed entity that can be activated and deactivated by investigators'*.
- 2016 warrant:** the section 30K report stated: *'The devices are permanently fixed in the prison, therefore no premises were entered for the purposes of the installation or retrieval of the warrant.'*
132. While we consider this to be a positive practice, given its isolated occurrence, we did not consider these to indicate the Court was aware of the integrated listening devices more broadly. Both warrants were issued by judges who did not issue any further prison-related warrants; and the circumstances of each were confined to specific areas of specific prisons. On no occasions did a report clearly state a device was originally installed without the authority of a warrant.
133. Between 2009 and 2016, there were a further 55 warrants issued relating to prisons. In all cases, the report to the issuing judge made no reference to the permanent installation of a device.

134. These are the only references to the permanent installation of a device in records we inspected.³² We note there is a possibility that warrant applications prior to 2008 may refer to the integrated listening devices; however, we have no indication from Victoria Police this is the case.

Recommendation

Recommendation 5

To provide transparency to the judge or magistrate, and enable effective oversight of their use of surveillance devices, Victoria Police revise its process for section 30K reporting to be clear on the nature of any installation and activation of a surveillance device, and to accurately report on the date and time a device was activated where the use of the device is restricted (such as to coincide with the presence of the person under investigation).

This approach should apply more broadly than solely on the use of surveillance devices in prisons: active consideration should be given to ensuring the section 30K reports provide an accurate picture of the use of surveillance devices under any warrant.

Victoria Police's response: accepted.

Finding 9: Victoria Police records on management of privacy

Outline

135. The activation of surveillance devices to accord with the presence of the person under investigation was a fundamental aspect of the issue that arose in Tasmania. It was also a key consideration for our inspection, particularly given the significant number of integrated listening devices in Victorian prisons.

Finding 9

Assessment

If an integrated listening device was activated, was it only active at times the target was present or activated on an ongoing basis?

Were any such activations consistent with the warrant and the explanation of how privacy would be managed as described in the affidavit?

³² We identified one instance for a separate 2016 warrant where the TSU informed the area administering the warrants, the SPU, that "Devices in these locations are never 'removed'".

Finding

We were unable to definitively verify whether activations of the integrated listening devices were consistent with warrants due to the unavailability of primary records that indicated when these devices were activated.

We made **1 recommendation** about practices to improve record-keeping in this area.

The recommendation is provided in full at the end of this section.

136. For one quarter of the warrants, the section 30K report provided the specific days on which a device was activated. This indicated to us that the device was at least activated on a day the person under investigation was present.
137. In the remaining instances where a device was activated, only the period the device was active (i.e., able to be used) was listed, which was typically the period between install/activation and retrieval/deactivation. This did not provide a clear data point for assessing compliance with the parameters of the warrants.
138. Unfortunately, due to several factors, which included issues with its surveillance device logging system, Victoria Police did not have records which we could use to verify that surveillance devices were only activated at the appropriate times.
139. For example, where a report stated a listening device was activated on a particular day, there were no records which we could use to confirm the surveillance device was used on that day or only at a particular time. There were also no records from which we could correlate activations to times when the target was present.
140. While we consider that records detailing activations on specific days indicate a level of compliance with the warrant, we cannot definitively determine that devices were activated only at the appropriate times in all cases.
141. We understand that given the time that has now elapsed, there is little likelihood of such records now being made available.
142. For this reason, where the integrated listening devices were activated in the monitoring suites by investigators, we cannot provide a definitive assessment to confirm that activation of these devices complied with the parameters of a warrant.

Recommendation

Recommendation 6

Victoria Police to review its record-keeping process for surveillance devices so it keeps verifiable records that demonstrate the installation, activation, and deactivation of a surveillance device is consistent with the authority of a warrant.

For prisons, Victoria Police should also keep records to correlate the presence of the target and other specified persons with the activation of surveillance devices.

Victoria Police should report to IOV with a proposal that satisfies this recommendation by **30 January 2026**.

Victoria Police's response: accepted.

Finding 10: Victoria Police procedures

Outline

143. We reviewed Victoria Police's general policies and procedures relating to the use of surveillance devices, and its specific policies and procedures about the use of those within prisons. This was important to understand the policy basis for the integration of listening devices in prisons, and whether it was supported by procedures.

Finding 10

Assessment

What internal policies and procedures did the TSU have in place that address the activation or installation of surveillance devices in prisons?

Are there any other relevant policies or procedures that dealt with surveillance devices in prisons?

Did these reasonably support compliance with the SD Act?

Finding

While Victoria Police had some procedures, these did not cover all important aspects of the process.

We also found that Victoria Police's general policy and procedures did not appear to support the use of integrated listening devices.

We make **1 recommendation** so that Victoria Police incorporates the improvements recommended into procedures.

The recommendation is provided in full at the end of this section.

144. We found the TSU had procedures regarding the activation of integrated listening devices in prisons from 2018 onward. These were largely focused on logistical aspects of the activation process but otherwise appeared to be consistently applied.
145. We could not identify any other procedures that dealt with the use of integrated listening devices, such as procedures about how these should be referred to in warrant applications

or reported to judges, described in the ARS or to inspecting bodies, and what restrictions or requirements the use of monitoring suites by investigators was subject to.

146. Another factor we considered is how the integrated listening devices fit within Victoria Police's broader policy positions on the use of surveillance devices.

147. The earliest procedure available in our records was the Chief Commissioner's Instruction from 2006 on Surveillance Devices. As a document which was broadly available to police officers, this did not cover specific surveillance device methodologies. Additionally, however, it did not appear to support or contemplate a scenario where listening devices could be installed without a warrant. This same approach is applied in other various iterations of Victoria Police's procedures through to the present day.

Recommendation

Recommendation 7

Victoria Police to revise its surveillance device policies and procedures to account for the specific processes recommended in this report.

Victoria Police's response: accepted.

Findings 11-12: oversight engagement – transparency

Outline

148. As part of our inspections, we regularly include criteria about how the agency engaged with us, and whether they were cooperative and frank. We include this so each agency understands what we expect from them.

149. Given the historical nature of the issues addressed by the inspection, we also assessed transparency from the lens of previous inspections. That is, was the information provided during previous inspections indicative of the use of integrated listening devices – and by extension – what was possibly known by previous inspections teams.

Finding 11

Assessment

Did the records provided for prior inspections accurately reflect the installation and activation of surveillance devices in prisons?

Finding

We found that prior records reflected that some listening devices were activated and deactivated, and there were 2 reports and a

letter that indicated fixed or permanent devices in one prison location.

However, there was no clear indicator that would prompt inspecting officers to consider the possibility of a broader program of integrated listening devices installed without the authority of a warrant.

The records suggested that inspecting officers had assumed that any device activated under a current warrant was authorised by a prior warrant.

We make **1 recommendation** regarding proactive disclosure of new methodologies to ensure we are kept apprised of Victoria Police's use of surveillance devices.

The recommendation is provided in full at the end of this section.

150. One key area of interest to us during the inspection was why we were previously not aware of this methodology. Following the inspection, we compared our assessments to internal records kept from previous inspections dating back to 2008. Some prior records reflected the activation and deactivation of listening devices, but it did not appear there were any records to prompt direct consideration of the possibility these were installed without authority.
151. It appeared to us the previous inspecting officers had assumed, based on information presented to them, that the devices were installed under a preceding warrant and left 'in situ'.
152. For example, there are notes from 2011 by the SIM's inspecting officers which state (about a device in prison) '[...] *nothing in database in respect of retrieval so it looks like device was left in situ*'.
153. The closest reference to an active consideration of the integrated listening devices in prisons comes from a handwritten note of a meeting with the TSU in April 2012. This states, '*Unclear if device left in situ at end of the warrant. Discussion on how to report where devices left on prison premises for future use. Just switched off either remotely or on site. Further consideration reqd*'.
154. The inspection database record for this warrant states, '*Device in situ from previous [warrant], nothing on file to indicate device was retrieved [...]*'.
155. While we now understand these to be integrated listening devices, these notes suggest a belief that listening devices remotely activated were left in place at the cessation of a preceding warrant – rather than installed without a warrant at the time of prison construction or renovation.
156. A misapprehension about the origins of these devices appears to be reflected in other inspection notes at around the same time regarding 3 other warrants: '*Prison LD's [listening devices] are always complicated – clear that device was 'made available' – TSU forms state 'activated' and ER [effectiveness report] includes date of installation and dates of issue.*

Would be better for Report to also reflect this – that devices were installed between dates but no recording were made’.

157. In most cases, the database which records the inspection of these warrants between 2008 and 2024, adopted the terminology of the ARS: that the devices were *installed* and *retrieved*.
158. For our purposes, if the previous inspecting officers were aware of the integrated listening devices, there would be less uncertainty around what installation, retrieval, activation and deactivation meant.
159. We consider this suggests previous inspecting officers were not aware of the integrated listening devices – and would have no reason to suspect this was a practice.
160. As identified in Finding 8, there were 2 section 30K reports to judges that stated listening devices were permanently installed. We consider it important to understand how these were approached by previous inspecting officers.
161. For the first of those, which is a supplementary report to the judge which dates to 2010, the report had noted that *‘nil technical staff utilised as surveillance device is a fixed entity that can be activated and deactivated by the investigators’*. Early inspection records from the SIM about that report reflected *‘[...] supplementary report is dated 8 March 2010. Content in these reports is much more informative than previously provided.’*
162. The second indication is from a 2016 section 30K report which indicated *‘[t]he devices are permanently fixed in the prison, therefore no premises were entered for the purposes of the installation or retrieval of the warrant’*. Records from the 2017 inspection of this warrant reflect *‘inst: permanently installed’*.
163. While these references to fixed entities and permanent devices relate to the existence of integrated devices, considering the previous inspections officer’s apparent belief about the use of devices left ‘in situ’ for future use, it is most likely these were taken to be devices that were installed under a previous warrant and left permanently for future use. Consistent with this understanding, the inspection reports that covered the 2016 warrant stated Victoria Police was compliant.
164. Importantly, the records the previous inspection officers relied on for every other warrant that related to integrated listening devices had, in most cases, referred to the installation and retrieval of surveillance devices. This likely created a strong impression that devices were installed under warrant; a strong belief that would not be influenced by only 2 references that were made 7 years apart.
165. It is also important to note that for the first 6 years of its operation, there was no independent inspection framework in place under the SD Act. The oversight framework and inspection function of the SIM became operative on 1 July 2006. This function was then assumed by the then Victorian Inspectorate in 2013.
166. This meant many integrated listening devices in prisons were operative prior to the oversight framework, and the practices around how the use of such devices were reported was likely already well established.

167. Victoria Police's response to this report asked for acknowledgement that the Supreme Court and IOV were informed of the fixed surveillance devices via the 2009 and 2016 section 30K reports and a letter to the Victorian Inspectorate dated 31 January 2018.
168. This letter referred to an installed device with recording capability and was sent by Victoria Police to request the Victorian Inspectorate's oversight of a rectification process over which we had no jurisdiction. It was not a disclosure about the installation of devices without authority and did not relate to Victoria Police's installation or use of the device.
169. Whilst we acknowledge the Victorian Inspectorate did not enquire about references to installed listening devices in the letter and the 2009 and 2016 section 30K reports, we do not accept Victoria Police's position that they constituted disclosures of the integrated listening devices covered by this report.

Recommendation

Recommendation 8

Where Victoria Police proposes or intends to use a new capability under the authority of the SD Act, that it proactively discloses this to IOV and considers providing any supporting legal advice.

Where relevant, similar disclosure processes should occur for the Courts and the PIM.

Victoria Police's response: accepted.

Finding 12

Assessment

Was Victoria Police cooperative and frank in dealing with IOV during the inspection?

Did they provide fulsome responses to any queries?

Did they provide access to all material and information in a timely manner?

Finding

We found that various areas of Victoria Police we engaged with during the inspection were helpful and assistive.

Given its ownership over the integrated listening device capability, we note the TSU was frank and open about its practices and provided a range of records that assisted our inspection.

170. During the inspection, we engaged with 3 areas of Victoria Police: the SPU, PSC and TSU. We found they were transparent and helpful throughout our inspection. We note they positively engaged with us during the inspection and showed a genuine intent to ensure Victoria Police was following the best practice approach to compliance and transparency.

171. The SPU and PSC were required to facilitate access to the warrant files. Given the age of some of these files, these were retrieved from Victoria Police's deep storage facility. Both areas provided timely access to the materials we required and were helpful during the inspection.

172. The TSU were required to provide a range of documents that evidenced the actions taken in relation to the integrated listening devices. We found the TSU undertook extensive preparation for the inspection, including identifying appropriate documents which detailed the activation and use of the integrated listening devices. The TSU's positive engagement and assistance during the inspection was integral to informing our understanding of the actions taken in relation to these warrants between 2008 and 2024.

Victoria Police's position

173. For procedural fairness, Victoria Police was provided with an opportunity to comment on the findings and recommendations contained in this report prior to its finalisation. Victoria Police's feedback was incorporated into various parts of the report, as appropriate.

174. The following dot points relate to matters that Victoria Police wishes to be acknowledged with respect to the report's findings:

- the integrated listening devices were only ever activated under the authority of a valid warrant
- Victoria Police obtained guidance which confirmed its belief that its use of the integrated listening devices, dating back to 2001, was lawful
- no use was made of material containing Legal Professional Privilege
- immediately after becoming aware that the use of the integrated listening devices may have been inappropriate, Victoria Police terminated their use
- Victoria Police indicated that many of the concerns raised in the report were a direct result of its use of the integrated listening devices to conduct surveillance, and if it had not used these devices many of these concerns would not have arisen.

175. Victoria Police also wishes it to be acknowledged that throughout the last two years it has consistently engaged with IOV since enquiries were first made in July 2023; and during that time, it has:

- provided additional information requested by IOV in five separate letters (a sixth letter was provided on 13 October 2025) within the time frame requested by IOV unless an extension was sought due to staff absences or because they were awaiting external guidance
- sought external guidance for all questions asked by IOV, regardless of their confidence in their proposed answer
- attended a number of meetings with IOV whereby detailed information was provided and presented to IOV staff ensuring timely and transparent responses to questions could be facilitated (for example the PPT Presentation on integrated listening devices on 1 November 2024) and
- expended considerable resources undertaking the above.

176. As part of its final response, Victoria Police also reiterated that it has always acted in good faith and in accordance with the guidance it received and only activated integrated listening devices under the authorisation of a valid warrant. Victoria Police also noted that it acted immediately upon becoming aware and receiving further guidance regarding concerns that use of integrated devices may have been inappropriate.

Glossary

Key terms	
30K Report	A report under section 30K of the SD Act made by the applicant or person primarily responsible for executing the warrant that is given to a judge who issued the warrant. It provides details about the use and information obtained by the authorised surveillance device(s)
ARS	Action Report Sheet, a document made by the Technical Surveillance Unit that details the actions taken by its officers to execute the warrant, e.g., install, maintain or retrieve a surveillance device
APS	Affidavit Preparation Section, a section of Victoria Police that prepares affidavits for surveillance device warrant applications
ESD	Ethical Standards Department, the predecessor to Professional Standards Command
Integrated listening devices	Listening devices and their supporting equipment permanently installed in prisons by Victoria Police
Interpose	A case management system used by Victoria Police to store and transmit law enforcement data
IOV	Integrity Oversight Victoria
Listening device	Any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear
PIM	Public Interest Monitor, whose function includes appearing at a hearing of an application for a surveillance device warrant to test the content and sufficiency of information relied on and the circumstances of the application

PSC	Professional Standards Command, the Victoria Police command responsible for promoting ethical standards and investigating misconduct or corrupt behaviour by police
TSU	The Technical Surveillance Unit, the area of Victoria Police responsible for installing and managing surveillance devices
SD Act	<i>Surveillance Devices Act 1999</i>
SIM	Special Investigations Monitor, the inspecting body for surveillance device warrants between 2006 and early 2013
SPU	Special Projects Unit whose responsibilities include administering most of the surveillance device warrants issued to Victoria Police
Surveillance device	A device that may capture the conversations, activities or geographical location of a person - including a data surveillance device, a listening device, an optical surveillance device or a tracking device; or a device that combines these types of devices
Warrant	A warrant authorising the covert use of surveillance devices under the SD Act.