
Inspection Report:

Surveillance Devices Act 1999 (Vic)

Report on irregular inspection of IBAC surveillance device records by the Victorian Inspectorate in May-June 2023

Contents

Executive Summary	3
Introduction and overview of our functions	4
Inspection Results.....	5
INSPECTION DETAILS.....	5
FINDING 1 – SURVEILLANCE DEVICE WARRANT AFFECTED BY SWEARING IN ISSUE	5
FINDING 2 – TRANSPARENCY TO THE PUBLIC INTEREST MONITOR	7
FINDING 3 – EFFECTIVE SELF-DISCLOSURE MECHANISMS	8
FINDING 4 – PROCEDURES GUIDING QUARANTINING PROCESSES.....	10
FINDING 5 – USE AND COMMUNICATION RECORDS.....	12
FINDING 6 – FULL AND FREE ACCESS	13

Executive Summary

1. In September 2022, the Independent Broad-based Anti-corruption Commission (IBAC) disclosed a delegation error to the Victorian Inspectorate (VI) where certain IBAC Officers, including 12 investigators, had not been sworn in by a person delegated to do so (**swearing in issue**). This affected some functions that could be performed by these IBAC Officers during the period 12 August 2021 to 26 August 2022, including an application for one surveillance device warrant. This warrant had not been executed at the time the issue was discovered by IBAC.
2. Subsequently, on 6 April 2023, IBAC disclosed a further compliance issue which affected the information used in support of the application for the same surveillance device warrant. This warrant was not executed, and in any case, had been determined to be invalid by the issuing authority in September 2022 as a result of the swearing in issue when IBAC sought to revoke the warrant.
3. Due to the broader risks associated with the use of information obtained under a surveillance device warrant affected by a compliance issue, and the apparent recurrent historical compliance issues, the VI determined to further assess whether actions taken by IBAC in relation to surveillance device warrants were appropriately delegated and/or authorised.
4. As a result of this surveillance devices inspection, the VI made **5 recommendations** to IBAC to address identified compliance issues. All of these have been accepted by IBAC, as outlined in the body of the report.
5. The VI welcomed IBAC's positive engagement on this inspection report and notes the Commissioner's commitment to fostering a culture of openness and transparency.
6. We have also made **2 suggestions**, which have been noted by IBAC.

Introduction and overview of our functions

7. The *Surveillance Devices Act 1999* (Vic) (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 the use of surveillance devices.
8. The SD Act provides the legislative framework for these agencies to use surveillance devices to investigate, or obtain evidence of the commission of, an offence that has been, is being, is about to be, or is likely to be, committed. Law enforcement officers of these agencies can apply to the Supreme Court for a surveillance device warrant authorising use of the following types of devices: data, listening, optical, and tracking.
9. For tracking devices only, an application may be made to the Magistrates' Court. Victoria's Public Interest Monitor (PIM) is entitled to make submissions on warrant applications. In addition to court-issued warrants, senior officers of Victoria Police and IBAC may, in certain emergency situations, authorise the use of surveillance devices. An application for approval to exercise powers under an emergency authorisation must be made to a Supreme Court judge within the following two business days.
10. The role of the VI is established by the SD Act, and it ensures independent oversight of agencies' compliance with the SD Act. The VI is required to inspect, from time to time, the records of each agency and report on the results of its inspections at six-monthly intervals to each House of Parliament as well as the Attorney-General. The use of surveillance devices by Victorian government agencies is highly intrusive, and therefore the VI's role is designed to independently assess the extent to which agency actions comply with the SD Act.

Inspection Results

INSPECTION DETAILS

11. The VI notified IBAC of its intention to conduct an inspection on 5 May 2023. The inspection took place on site at IBAC from 29 May to 1 June 2023. The VI engaged with IBAC on matters relevant to the inspection through to 6 June 2023. During the compilation of this report, the VI further engaged with IBAC from 17 July to 25 July 2023 to clarify elements of the inspection, including the background to the discovery of the swearing in issue.
12. Further background on the swearing in issue that gave rise to the inspection is detailed in **Finding 1** below.
13. The purpose of this inspection was to determine whether appropriate delegations, authorisations and approvals were in place when IBAC applied for surveillance device warrants.
14. Where required, the inspection also assessed whether IBAC had effective measures in place to ensure the compliant use and communication of information obtained under warrants, and processes to appropriately quarantine and manage any information affected by a compliance issue.
15. The VI inspected all surveillance device warrants that ceased within the period 1 January 2021 to 31 December 2022. This covered 11 issued warrants and 10 extensions of warrants.
16. This inspection was guided by a defined Inspection Criteria. These are set out at **Annexure A**.

FINDING 1 – SURVEILLANCE DEVICE WARRANT AFFECTED BY SWEARING IN ISSUE

Were appropriate delegations, appointments, or authorisations in place relating to surveillance device warrants?

Relevant legislation

17. Under section 37(1) of the *Independent Broad-based Anti-corruption Act 2011* (IBAC Act), before commencing employment with IBAC, a person referred to in section 35 of the Act must take an oath or make an affirmation. The Commissioner has the power under section 37(3) to administer the oath or affirmation and is authorised under section 32 to delegate this power.
18. Under section 15 of the SD Act, an application for a surveillance device warrant can only be made by a law enforcement officer. Under section 3(1) of the SD Act, a 'law enforcement officer' includes a prescribed IBAC Officer.¹ This is further defined as a sworn IBAC Officer within the

¹ A prescribed IBAC Officer is defined in the SD Act as a sworn IBAC Officer within the meaning of section 3(1) of the IBAC Act who holds a position, or is a member of a class, that is prescribed by the regulations. Under section 7 of the *Surveillance Devices Regulations 2016*, in force at the time, prescribed IBAC Officers are the Commissioner, Deputy Commissioners, the CEO, and IBAC Officers classified as Executive Officers, Senior Technical Specialists, or as non-executive employees Grade 4, 5 or 6.

meaning of section 3(1) of the IBAC Act; that is, an officer who has taken an oath or made an affirmation under the IBAC Act.

Background

19. On 9 September 2022, IBAC advised the VI that it had identified an error in its delegations for the authorisation of senior IBAC Officers to administer the oath or affirmation to new IBAC Officers. A change to delegations made on 12 August 2021 had removed the delegation for IBAC Directors to swear in new staff.
20. The power for IBAC Directors to swear in new IBAC Officers was delegated under an additional instrument that had not been considered at the time IBAC revoked this and made a new overarching instrument of delegation on 12 August 2021.
21. As a result of this error, from between 12 August 2021 to 26 August 2022, Directors continued to swear in staff without knowing they were no longer authorised to do so. This affected 12 investigators, as advised by IBAC, one of whom had applied for a surveillance device warrant.
22. The VI did not further review IBAC's processes for the management of its delegations, as this was outside the Inspection Criteria. As noted under other matters below, IBAC is separately taking additional actions to improve its management of delegations.

Table 1: Summary of delegation changes, issue of warrants and IBAC actions in relation to the swearing in issue

Date	Details
12 May 2021	IBAC delegates authority to Directors to swear in staff
12 August 2021	IBAC's new delegation and revocation of old delegations has the effect of removing authority for Directors to swear in staff. However, Directors continue to swear in staff.
16 August 2022	Affected surveillance device warrant issued
26 August 2022	Discovery of swearing in issue
9 September 2022	IBAC discloses swearing in issue to the VI
18 November 2022	The VI writes to IBAC seeking further information
14 December 2022	IBAC responds to VI's request with further details
12 January 2023	The VI writes to IBAC seeking further information
8 February 2023	IBAC responds to VI's request for further details
6 April 2023	IBAC makes further disclosure to the VI
5 May 2023	VI notifies IBAC of irregular inspection

Outcome and findings

23. During the inspection, the VI assessed 11 surveillance device warrants that ceased during the period 1 January 2020 to 31 December 2021. We also assessed 10 extensions to surveillance device warrants within the same period.
24. We confirmed, as reported by IBAC, that one surveillance device warrant issued on 16 August 2022 had been affected by the swearing in issue as the applicant had not been correctly sworn in under the IBAC Act. This warrant however had not been executed at the time the delegation issue was discovered by IBAC and no surveillance devices had been installed.

25. IBAC subsequently returned this warrant to the issuing authority for revocation on 6 September 2022. IBAC was advised that revocation was not necessary as the warrant had been invalid from the outset.
26. We did not identify any further warrants affected by this issue.
27. The application for this warrant at least partially relied on information affected by a further compliance issue disclosed to the VI on 6 April 2023. This is addressed at **Finding 2** below.

Other matters

28. IBAC advised in its 14 December 2022 letter that it intended to undertake a review of its delegations during 2023. It also noted that its Delegations Framework would be reviewed biannually to minimise the likelihood of a future delegation error, such as the swearing in issue.
29. We also note that, in its 6 April 2023 letter, IBAC advised it had recently commenced a review of its delegations register and would explore opportunities to streamline the process for drafting and updating instruments of delegation.
30. Subsequently, IBAC advised the VI during the inspection that all of its delegations are presently under review.

FINDING 2 – TRANSPARENCY TO THE PUBLIC INTEREST MONITOR

General finding

Relevant legislation

31. Under section 12C of the SD Act, an application must fully disclose to the PIM all matters of which the applicant is aware that are adverse to the application.

What we observed

32. As a result of the further compliance issue disclosed on 6 April 2023, IBAC had used information potentially affected by a compliance issue to support the application for a surveillance device warrant. This was the same warrant affected by the swearing in issue as noted above.
33. The affidavit made in support of the application for this surveillance device warrant made no reference to reliance on information obtained under a warrant that may be subject to a compliance issue. Whilst IBAC as an entity knew about the compliance issue, we note that there is nothing to indicate that the applicant was aware of this issue. The applicant had therefore unwittingly not disclosed this adverse matter to the PIM.
34. In this regard, we note that IBAC (via the applicant) had included a statement in the affidavit for this surveillance device warrant application that it had disclosed all matters favourable and adverse relevant to the application. While we acknowledge the applicant had acted in good faith, this statement was in effect inaccurate.

Our recommendations

35. Given the significant implications for accountability and transparency, as well as with regards to the functions of the PIM, we have made two recommendations.

Recommendation 1

We recommend that, if it has not done so already, IBAC inform the PIM that the application made in respect of a particular surveillance device warrant had omitted a matter that may have been adverse to the application, since it may have relied on information affected by a compliance issue.

Recommendation 2

We recommend that where an application relies on material from other warrants, applicants are required to confirm whether there are any adverse matters that should be disclosed by referring to IBAC's compliance issue register (see Recommendation 3 under Finding 3).

36. IBAC accepted both recommendations. Recommendation 2 was accepted on the basis that IBAC would consider how it could implement, and pilot, an interim measure with a view to assessing its effectiveness and suitability. This followed feedback from the VI that IBAC may acquit the intent of this recommendation through the keeping of a basic register or spreadsheet.

FINDING 3 – EFFECTIVE SELF-DISCLOSURE MECHANISMS

What mechanisms does IBAC have in place to ensure that it self-discloses issues to the VI in a timely manner?

Compliance principle

37. It is essential that an agency has effective processes in place through which it can track and act on compliance issues. This ensures that issues are acted on when they should be, and that the agency can transparently disclose known issues to an oversight body. Such a process can also act as a failsafe to mitigate against the loss of corporate knowledge where staff movements or turnover occurs.
38. In line with the above inspection criterion and compliance principle, we reviewed the policies and procedures that guide IBAC staff on when to report incidents and when to make disclosures to the VI. We also considered other mechanisms IBAC had to support timely self-disclosure of compliance issues.

What we observed

39. To assess how IBAC centrally tracks compliance issues, we sought confirmation on whether there was a central register or equivalent mechanism for this purpose. IBAC advised during the inspection that it does not currently keep such a register; however, it was developing a 'correspondence register' which will, among other things, record compliance issues reported by IBAC or identified by the VI.
40. Such a register, if supported by an appropriate policy, would represent a significant improvement to IBAC's processes and would mitigate the risk that an issue would not be acted on. This may ensure that, irrespective of staff movements or changes to organisational structure, the details of issues are readily available and centrally managed. This policy should also address which staff are responsible for the maintenance of the register, and when, and how, operational staff are to report issues.
41. During the inspection IBAC advised that there was no policy or procedure in place outlining when a disclosure should be made to the VI in relation to a potential compliance issue under the SD Act. We noted positive enhancements have been made to a draft version of a different procedure on the reporting of compliance issues and the notification of these to the relevant oversight body.² The VI considers that this should be replicated within IBAC's SD Procedure.
42. It would also be beneficial that in replicating this information within the SD Procedure, IBAC specifically address which bodies contraventions should be reported to, in addition to consideration of whether the PIM should be informed of any matters that may have affected, or were adverse to, a warrant.
43. As the overarching mechanism for reporting incidents, we also considered how IBAC's Incident Management and Reporting Policy supported its ability to self-disclose compliance issues.
44. The version in place at the time the authority to exercise warrants issue occurred, the Incident Management and Reporting – Policy (2020), broadly defined incidents as being '*any unplanned event that signals an opportunity to improve, or creates or exposes IBAC to threats or hazards. This includes areas such as information management and security, physical and personnel security, property and assets, and **legal compliance.***' [emphasis added]
45. The VI also considers that it would be beneficial that reference is made within the examples under the definition of General Incident (previously Reportable Incident³) to include express reference to legal compliance issues, particularly for areas subject to oversight by independent bodies.

² The details of this procedure have been included in a separate report to IBAC.

³ The incident management policy was revised in August 2022 to make several updates, including redefining general and Occupational Health and Safety incidents.

Our recommendation

Recommendation 3

We recommend that to support disclosure and management of compliance issues, IBAC:

- 3.1 address legal compliance issues within the definition of a General Incident in its Incident Management and Reporting Policy and Procedure, particularly with reference to areas subject to independent oversight
- 3.2 formalise within its Surveillance Device Warrants Procedure a process for keeping a Register of Compliance issues which should make clear which staff are responsible for its maintenance and when, and how, operational staff are to report issues
- 3.3 to clearly identify within its Surveillance Device Warrants Procedure the bodies to which compliance issues must be reported, including a benchmark timeframe for when an initial disclosure should be made and a requirement that consideration be given to whether a disclosure to the PIM should be made.

46. IBAC accepted this recommendation and noted that due to its breadth it would require time to scope and implement the recommendation.

FINDING 4 – PROCEDURES GUIDING QUARANTINING PROCESSES

Has IBAC appropriately managed and quarantined any information obtained under or relating to a warrant affected by a compliance issue?

Relevant compliance principle

47. Under Criterion 3, we assessed the measures IBAC had in place to quarantine and prevent the further use and communication of information obtained under a surveillance device warrant affected by a compliance issue. We also assessed whether these measures were sufficient to ensure compliance.
48. In line with Criterion 3, we also assessed that where a surveillance device warrant was affected by a compliance issue, that information had been appropriately quarantined (including information which had been used or communicated).

What we observed

49. In line with the above criteria, we sought to verify the processes IBAC had in place to quarantine any information obtained under a warrant affected by a compliance issue. This includes information obtained under SD warrants and other documents that may incorporate this information, such as affidavits.
50. As the one affected surveillance device warrant was not executed, it was not necessary to confirm that any information obtained had been quarantined. However, as the application for

this warrant contained information connected to the further delegation issue, we sought to confirm that access to any documents containing this information had been restricted.

51. During the inspection, through our access to IBAC's record-keeping system, we observed that no affidavits or other documents containing information obtained under an affected warrant had been quarantined from further access. We also note there were no markings associated with these documents to indicate that they contained information that otherwise should have been subject to quarantine.
52. While we note that access to these folders is restricted to certain IBAC staff, to prevent further use or communication of this information it is important that access be restricted to the maximum possible extent and for records to be clearly marked as being subject to quarantine.
53. Based on advice provided during the inspection, it appears IBAC had not turned its mind to the need to quarantine information relating to the application for, and issuance of, the warrant.
54. We have also addressed the clarity of IBAC's records where information is used internally under **Finding 5** below.

Our recommendation and suggestion

55. To ensure it effectively quarantines information relating to a surveillance device warrant, as the need arises, IBAC should document its process for quarantining records into policy and procedure, in line with the below recommendation.

Recommendation 4

We recommend that IBAC address quarantining of information obtained under warrants within its Surveillance Device Warrants Procedure. This includes setting out the process for quarantining data collected under warrants, as well as managing other documents that contain warrant-related information such as affidavits.

This process should seek to clearly identify any documents or records that contain affected material and aim to limit any further access to the maximum extent possible.

Suggestion 1: For the purpose of restricting access to documents that contain information subject to quarantine, the VI also strongly suggests that IBAC develop a process checklist. The requirement to complete the checklist for quarantining information, as well as the nominated officers responsible for using it, should be outlined in IBAC's Surveillance Device Warrants Procedure.

56. IBAC accepted this recommendation and noted our suggestion.

FINDING 5 – USE AND COMMUNICATION RECORDS

Does IBAC have appropriate and effective procedures and policies in place to ensure that use or communication of information obtained under surveillance devices is compliant?

Relevant legislation and practice

57. Under section 30N(c) of the SD Act, IBAC is required to keep details of each use of information obtained from a surveillance device by an IBAC Officer.
58. Under section 30N(d) of the SD Act, IBAC is required to keep details of each communication by an IBAC Officer of information obtained from a surveillance device to a person other than an IBAC Officer.
59. IBAC satisfies these requirements by keeping a master spreadsheet for each particular operation and type of warrant/authorisation.

What we observed

60. In accordance with our inspection criteria, we assessed whether IBAC had appropriate and effective procedures in place to ensure the use and communication of information obtained from a surveillance device was compliant with the SD Act.
61. Since the affected surveillance device warrant had not been executed, no information had been obtained. For other surveillance warrants we inspected, whilst we found IBAC kept sufficient records of communications, we nonetheless observed that improvement is necessary to ensure that IBAC accurately captures the details of each use within its registers.
62. We have not previously commented on this from our regular inspections of surveillance device records, since at these inspections we assessed only whether use was recorded and whether this was consistent with the statutory reports.
63. In several instances, IBAC recorded only a general statement that did not clearly reflect the details of each use. Noting the SD Act requires IBAC to keep details of *each* use, we were not able to accurately assess whether IBAC had met these requirements, given the general nature of the use recorded.
64. We also note that in some instances, there was no end-date recorded for the use. This reduced clarity as to the nature of the use and when it had occurred. We understand there are practical limitations that make it difficult to record each and every use; however, the VI is of the view that improvements on this point are needed to ensure IBAC clearly demonstrates it meets the requirements of the SD Act.
65. Where there is limited information available as to how information has been used, we may be unable to assess whether the use was for a permitted purpose. For that reason, it is important that IBAC's registers are sufficiently detailed.

Our suggestion

Suggestion 2: We suggest that IBAC provide further guidance to staff so that greater detail is given in entries made to its registers. This will ensure IBAC can clearly demonstrate it has met the requirement to keep details of *each* use of information obtained from a surveillance device.

66. IBAC noted our suggestion and sought the VI's support to provide training to IBAC Officers on expectations for managing entries in its SD registers. The VI indicated that we were open to providing a presentation to IBAC Officers on our inspections and other functions, including commonly identified issues, within the next financial year.

FINDING 6 – FULL AND FREE ACCESS

Was the agency transparent and cooperative with the VI?

Relevant legislation

67. Under section 30P(2)(b) of the SD Act, the VI is entitled to have full and free access at all reasonable times to all records of the agency that are relevant to the inspection.

What we observed

68. During the inspection, IBAC's compliance team was helpful and responsive in addressing our questions.

69. We note that while we had requested audit-level access to IBAC's corporate records system, the access available to inspection staff was limited to records made available by IBAC. In cases where we sought additional records from IBAC, each record had to be requested and provided on an individual basis, rather than the VI having access to search for records it considered relevant.

70. While IBAC was responsive in providing these records, noting IBAC had advised the VI of resourcing concerns prior to the inspection, these access restrictions may have further increased IBAC's workload to facilitate the inspection. For our regular surveillance device inspections, we have been satisfied with the level of access provided. However, given the nature of this inspection, which covered various elements of IBAC's surveillance device warrant framework, this limited access was not suitable.

Our recommendation

Recommendation 5

We recommend that IBAC revises its approach to facilitating access during inspections to ensure that the VI is appropriately afforded full and free access to all relevant systems.

71. IBAC accepted this recommendation on the basis that the Memorandum of Understanding between the VI and IBAC will include a provision that addresses this recommendation.

Annexure A

Inspection criteria related to surveillance device warrants: IBAC irregular inspection, covering records for the period 1 January 2021 to 31 December 2022⁴

Criteria	Methodology
1. Were appropriate delegations, appointments, or authorisations in place relating to surveillance device warrants?	
What delegations and authorisations did IBAC have in place for the period relevant to the application for and exercise of powers under warrants and did these authorise the necessary actions?	Assessments in the following areas: Register of delegations, instruments and authorisations IBAC records-management system
Was each surveillance device warrant application made with the approval of a senior officer of IBAC? (s 9 of the Surveillance Device Regulations 2016 and s 15(2)(a) of the SD Act) (as defined in s 3(1) of the SD Act and prescribed in s 7 Surveillance Devices Regulations 2016)	Record checks in the following areas: SD warrant applications SD warrant affidavits Internal approval of application for an SD warrant Acting appointments and HR records for officers acting in such positions
Was each prescribed IBAC Officer who applied for a surveillance device warrant a properly sworn IBAC Officer? (s 7 Surveillance Devices Regulations 2016; s 3(1) and s 37 IBAC Act)	Record checks in the following areas: SD warrant applications SD warrant affidavits Acting appointments and HR records for officers acting in such positions
What training, procedures and policy does IBAC have in place that supports awareness of relevant obligations when applying for and exercising warrants?	Assessments in the following areas: Policies and procedures Training documents Intranet information Inbuilt controls within Condor workflows
Are quality assurance measures sufficient to identify any compliance issues with applications for warrants, particularly in relation to the approval and delegation of persons?	Assessments in the following areas: Policies and procedures Templates, review (quality assurance) checklists and documents Process discussions with staff
2. Does IBAC have appropriate and effective procedures and policies in place to ensure that use or communication of SD information is compliant?	
What policy and procedures does IBAC have in place regarding the use and communication of information obtained under an SD warrant?	Assessments in the following areas: Policies, procedures, training, and related reference materials Process discussions with staff

⁴ Several formatting and typographical errors have been corrected with the criteria that was originally notified to IBAC. No substantive change has been made to the criteria.

Are these sufficient to ensure compliance?	
<p>IF AFFECTED BY A COMPLIANCE ISSUE:</p> <p>Do use and communication records provide sufficient information to identify the particulars of the use and communication of SD information, including when and how it was made? (ss 30N(c) and (d) of the SD Act)</p> <p>Are such records sufficient to determine compliance with ss 30N(c) and (d)?</p>	<p>Records checks in the following areas:</p> <p>Use and communication logs</p>
<p>IF AFFECTED BY A COMPLIANCE ISSUE:</p> <p>Do records provide details of each occasion when SD information was used in evidence in a relevant proceeding? (s 30N(e) of the SD Act)</p> <p>Are such records sufficient to determine with s 30N(e)?</p>	<p>Records checks in the following areas:</p> <p>Use and communication logs</p>
3. Has IBAC appropriately managed and quarantined any information obtained under or relating to a warrant affected by a compliance issue?	
<p>Where an SD warrant is affected by a compliance issue, what measures and procedures does IBAC have in place to quarantine and prevent the further use or communication of affected information?</p> <p>Are these sufficient to ensure compliance?</p>	<p>Record checks in the following areas:</p> <p>Use and communication logs</p> <p>TRIM audit trails and access permissions</p> <p>Affidavits</p> <p>Examinations</p> <p>Other related materials that make use of SD information</p> <p>Process discussions with staff</p>
<p>Where an SD warrant is affected by a compliance issue, has information been appropriately quarantined, including information that was used or communicated?</p>	<p>Record checks in the following areas:</p> <p>Use and communication logs</p> <p>TRIM audit trails and access permissions</p> <p>Affidavits</p> <p>Examinations</p> <p>Other related materials that make use of SD information</p> <p>Process discussions with staff</p>
4. Was the agency transparent and cooperative with the VI?	
<p>Was the agency cooperative and frank?</p> <ul style="list-style-type: none"> - What mechanisms does IBAC have in place to ensure that it self-discloses issues to the VI in a timely manner? - Did IBAC provide access to all relevant material in a timely manner? 	<p>Qualitative assessment based on engagement and provision of records.</p>