COMMONWEALTH OMBUDSMAN

Report to the Minister for Home Affairs on agencies' compliance with the *Surveillance Devices Act 2004* (Cth)

For the period 1 January to 30 June 2020

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 July to 31 December 2019

AUSTRALIAN FEDERAL POLICE
Records from 1 July to 31 December 2019

Report by the Commonwealth Ombudsman,
Michael Manthorpe PSM,
under s 61 of the *Surveillance Devices Act 2004* (Cth)

September 2020

COMMONWEALTH OMBUDSMAN

Report to the Minister for Home Affairs on agencies' compliance with the *Surveillance Devices Act 2004* (Cth)

For the period 1 January to 30 June 2020

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 July to 31 December 2019

AUSTRALIAN FEDERAL POLICE
Records from 1 July to 31 December 2019

Report by the Commonwealth Ombudsman,
Michael Manthorpe PSM,
under s 61 of the *Surveillance Devices Act 2004* (Cth)

September 2020

ISSN 2209-752X (Online)

ISSN 2209-7511 (Print)

Contact us

Enquiries regarding the licence and any use of this report are welcome at:

Commonwealth Ombudsman

GPO Box 442

Canberra ACT 2601

Tel: 1300 362 072

Email: ombudsman@ombudsman.gov.au

Contents

Overview

This report presents the results of the Office of the Commonwealth Ombudsman's (the Office) inspections conducted under the *Surveillance Devices Act 2004* (Cth) (the Act) during the period from 1 January to 30 June 2020 (the inspection period).

During the inspection period we conducted inspections of the Australian Criminal Intelligence Commission (ACIC) and the Australian Federal Police (AFP). We had planned to conduct inspections of the Australian Commission for Law Enforcement Integrity (ACLEI) and the Western Australia Police Force during this inspection period, but these were delayed due to the COVID-19 pandemic. We will include a sample of records from this period in our next inspection at both agencies.

Under the Act, specified law enforcement agencies can covertly use surveillance devices when investigating certain offences. This power is given to specific Commonwealth agencies for the purposes of combating crime and protecting the community. The Act also allows specified state and territory law enforcement agencies to use surveillance devices to investigate certain Commonwealth offences and enforce Family Court recovery orders.

The Ombudsman provides independent oversight by periodically inspecting the records of agencies that have exercised Commonwealth surveillance device powers. At these inspections, we assess whether the agency's records demonstrate it was compliant with the Act during the six months prior to the inspection period and, more generally, had processes in place to support compliance. We also consider the agency's transparency and accountability, and encourage it to disclose systemic problems or instances of non-compliance to the Office. If we identified problems at an agency during a previous inspection, we review any action it has subsequently taken to address these issues.

The most significant issues we identified during this inspection period were:

- agencies retrieving surveillance devices without clear and proper authority
- agencies seeking or authorising extensions to warrants not being sought or authorised in a manner compliant with the Act.

We also identified a number of reporting errors and records management issues.

Both agencies were responsive to our findings and actively disclosed instances of non-compliance to us, either when they arose or at the time of our inspection.

Introduction

The Act regulates law enforcement agencies' use of surveillance devices and access to data held in computers. Under s 6 of the Act, a 'surveillance device' means:

- a data surveillance device
- a listening device
- an optical surveillance device
- a tracking device
- a device that is a combination of any two or more of the above.

A 'computer' is defined under s 6 of the Act as one or more, or a combination of computers, computer systems and computer networks.

The Act allows law enforcement agencies to covertly conduct certain surveillance or computer access activities under a warrant issued by an eligible judge, a nominated Administrative Appeals Tribunal (AAT) member, an internally issued authorisation or, in limited circumstances, without formal authority.[1]

The Act imposes requirements for agencies to securely store and destroy information they obtain by using surveillance devices or through computer access activities. These types of information and records are collectively referred to as 'protected information'.[2] The Act restricts the way such information may be used, communicated or published, and imposes reporting obligations for law enforcement agencies to account for their covert surveillance device activities.

What we do

The Ombudsman performs the independent oversight mechanism set out in the Act. The Ombudsman is required to inspect the records of each law enforcement agency to determine the extent of its compliance with the Act and report the results to the relevant Minister every six months.

Why we oversee agencies

The covert use of surveillance devices or access to data held in computers by law enforcement agencies is highly intrusive. This is why the Ombudsman's oversight role

---

1 Part 4 of the Act provides the circumstances in which certain surveillance devices may be used without a warrant, for example, the use of an optical surveillance device where that use does not involve entry onto premises without permission.

2 Section 44 of the Act.

is important: we ensure these powers are used in accordance with the Act and, where this does not occur, hold agencies accountable. The Ombudsman's reporting obligations under the Act provide transparency to the Minister and the public about the use of these intrusive powers.

How we oversee agencies

The Office has inspection methodologies that it applies consistently across all agencies. These methodologies are based on legislative requirements and best practice standards, which ensures that all agencies are held to the same standard. We focus our inspections on areas of high risk, taking into account the likelihood and impact of non-compliance in particular areas and the relevant agency's past compliance record.

We assess compliance based on the records the agency makes available to us, discussions with relevant staff, observations of the agency's processes, and the efficacy and timeliness of the agency's actions to address issues we or its staff identify. To maintain the integrity of active investigations, we do not inspect records relating to warrants and authorisations that are still in force.

To ensure the agency understands what we assess, prior to each inspection we provide it with a broad outline of our criteria. This helps agency staff to identify the most accurate sources of information to assist our inspection. We also encourage agencies to disclose instances of non-compliance, including any remedial action they have taken.

At the end of each inspection we convene a meeting with relevant agency staff to discuss our preliminary findings. This enables the agency to commence remedial action without waiting for our report. We may also provide the agency with feedback on their policies and procedures, including communicating 'best practice' approaches to demonstrating compliance, and engage with staff about compliance issues outside the formal inspection process.

Our criteria

The objective of our inspections is to assess the extent of compliance with the Act by the agency and its law enforcement officers.

We use the following broad criteria to assess agency compliance:

1. Were surveillance devices used in accordance with the Act?
2. Were computer access activities conducted in accordance with the Act?
3. Is protected information properly managed?

4. Was the agency transparent and were reports properly made?

Further detail on our inspection criteria and methodology is provided in **Appendix A.**

How we report to the Minister

To ensure procedural fairness, we give each agency the opportunity to comment on our draft inspection findings. Once we have considered and, where appropriate, incorporated the agency's response, we finalise our inspection results. The findings from these reports are then desensitised and consolidated into the Ombudsman's six-monthly report to the Minister.

We may also report on matters that do not relate to specific instances of non-compliance, such as the adequacy of an agency's policies and procedures to demonstrate compliance with the Act. However, we will not generally include administrative issues or instances of non-compliance where the consequences are negligible.

Australian Criminal Intelligence Commission

From 10 to 13 February 2020 we conducted an inspection of the Australian Criminal Intelligence Commission's (ACIC) surveillance device records.

Inspection details

We inspected records of warrants and authorisations that expired during the period from 1 July to 31 December 2019 (the inspection period).

Inspection statistics		
Type of record	**Records made available**	**Records inspected**
Surveillance device warrants	57	19 (33.3%)
Computer access warrants	1	1 (100%)
Retrieval warrants	4	4 (100%)
Tracking device authorisations	12	9 (75%)
TOTAL	**74**	**33 (44.6%)**

Progress since our previous inspection

We last publicly reported inspection results for the ACIC in our March 2020 report to the Minister. In that report we identified that the ACIC had not completed its destruction of protected information as soon as practicable, as required under s 46(1)(b)(i) of the Act. We made two suggestions about the ACIC's destruction processes and committed to monitoring this issue at future ACIC inspections.

The ACIC did not make any destruction authorisations during the current inspection period.

In our last report we noted that the ACIC disclosed one instance where it quarantined data it had obtained in contravention of a condition on the warrant. Our inspection of this record identified that details about the disclosure were not included in the report the ACIC provided to the Minister under s 49 of the Act. We suggested the ACIC amend its report to the Minister to provide this additional information. At this

inspection, the ACIC advised it would correct the record in its next addendum to the Minister, which was due by 28 February 2020. We will review the ACIC's update to the Minister at our next inspection.

Inspection findings

At this inspection we identified a small number of instances of non-compliance that we considered to be administrative or low-risk in nature. These are explained below.

Disclosure—Warrants requested to be revoked but expired prior to revocation

What the Act requires

Under s 20(2) of the Act, the chief officer must revoke a surveillance device warrant if the prescribed circumstances in s 21 of the Act apply. Section 21(2) of the Act provides that if the chief officer is satisfied that the use of the surveillance device under the warrant is no longer necessary for the purpose of enabling evidence to be obtained regarding the commission of a relevant offence or the identity or location of an offender, then the chief officer must revoke the warrant.

What the ACIC disclosed

The ACIC disclosed seven instances where it had made requests to revoke surveillance device warrants, but those warrants expired prior to the chief officer making the revocation. This was caused by the ACIC making requests for revocation on the same day the warrant was due to expire or the appropriate revoking officer of the agency not being available. At the time of our inspection, the ACIC was updating its Surveillance Device Procedure to address this issue. We will review the ACIC's progress at our next inspection.

Disclosure—Retrieval warrants not revoked upon device retrieval

What the Act requires

Under s 27(2) of the Act, if the chief officer is satisfied that the grounds for issuing a retrieval warrant no longer exist, then the chief officer must revoke the warrant.

Section 27(5) of the Act provides that, if the law enforcement officer to whom a retrieval warrant has been issued, or who is primarily responsible for executing a retrieval warrant, believes the grounds for issue of the warrant no longer exist, they must inform the chief officer immediately.

What the ACIC disclosed

The ACIC disclosed three instances where it had not revoked retrieval warrants when it retrieved the device, contrary to s 27(2) of the Act. The ACIC advised that this issue would be an area of focus in its compliance activities and it had developed an enhancement to its case management system that will mitigate the risk of recurrences. We will review the ACIC's progress on this issue at our next inspection.

Finding—Protected information certified for retention after being certified for destruction

What the Act provides

Under s 46(1)(b)(i) of the Act, the chief officer must cause the destruction of any record or report comprising protected information as soon as practicable if satisfied that no civil or criminal proceeding to which the material relates has, or is likely to be, commenced and that the material is not likely to be required in connection with an activity or purpose prescribed under the Act.

Under 46(1)(b)(ii) of the Act, the chief officer must cause the destruction of any record or report comprising protected information within five years after the record or report is made, unless before the end of that period they are satisfied the material is required under a matter referred to at s 46(1)(b)(i) of the Act.[3]

What we found

We identified a number of records that the ACIC had certified for destruction but not yet destroyed and which it subsequently certified for retention. The ACIC advised that in these instances it identified, after the destruction was authorised, that the protected information was required for a purpose set out in s 46(1)(b)(i) of the Act. As such it sought a retention certification for the relevant records.

The ACIC delegate who certified that the protected information should be retained was made aware that the records had previously been authorised for destruction. While we do not consider these instances to be non-compliant, they highlight the risk of destroying evidence that is required if destruction authorisation processes do not also consider the retention provisions.

[3] For example, the material is required to make a decision on whether to prosecute a relevant offence or as evidence in a proceeding.

What we suggested

We suggested to the ACIC that, as a matter of better practice, it consider measures to ensure that, prior to authorising destruction, due consideration is given to whether protected information is likely to be required for a purpose set out in s 46(1)(b)(i) of the Act.

The ACIC's response

In response to this finding the ACIC advised that it would implement measures to support better decision making about certifying records for destruction. These measures will include improved guidance for staff about roles, responsibilities and required considerations for destroying protected information.

Australian Federal Police

From 2 to 6 March 2020 we conducted an inspection of the Australian Federal Police's (AFP) surveillance device records.

Inspection details

We inspected records of warrants and authorisations that expired during the period from 1 July to 31 December 2019 (the inspection period). We also inspected records relating to the AFP's management of protected information during these periods.

Inspection statistics		
Type of record	**Records made available**	**Records inspected**
Surveillance device warrants	297	40 (13.5%)
Computer access warrants	7	6 (85.7%)
Retrieval warrants	5	5 (100%)
Tracking device authorisations	85	20 (23.5%)
Destructions of protected information	306	33 (10.8%)
Retentions of protected information	35	22 (62.9%)
TOTAL	**735**	**126 (17.1%)**

Progress since our previous inspections

We last publicly reported inspection results for the AFP in our March 2020 report to the Minister. At that time we reported a number of compliance issues, including regarding tracking device authorisations. These included instances where the AFP:

- made an application for a tracking device authorisation instead of a retrieval warrant

- made a tracking device authorisation in circumstances that did not relate to the investigation of a relevant offence
- inaccurately reported to the Minister whether a tracking device authorisation was executed.

We did not identify further instances of these issues during the inspection period.

In our previous report we also referred to instances where the AFP:

- retrieved tracking devices without express authority
- sought, and authorised extensions to, warrants in a manner that did not comply with the Act.

We identified these issues again during our March 2020 inspection, discussed below.

At this inspection we also reviewed an additional instance of unauthorised extraterritorial use of a surveillance device. The AFP disclosed two instances to us at the time of our previous inspection but the records related to two different periods so were reviewed separately; one at the previous inspection and one at our March 2020 inspection. Our analysis to date indicates this is not a systemic issue, but we will continue to monitor the AFP's compliance with its extraterritorial obligations at future inspections.

Inspection findings

The most significant issues we identified during the inspection period were:

- tracking devices being retrieved without proper authority
- deficiencies in the AFP's approach to applying for, and maintaining appropriate records relating to warrant extensions.

As at previous inspections of the AFP, we also identified a small number of errors or omissions in its reports to the Minister under s 49 of the Act.

Finding—Evidence of extension and compliance with s 19(5) of the Act

What the Act requires

Section 19(2) of the Act requires that extension applications are made to an eligible Judge or nominated AAT member and accompanied by the original warrant. Under s 19(5) of the Act, if the eligible Judge or nominated AAT member grants the application, the Judge or member must endorse the new expiry date or the other varied term on the original warrant.

What we found

In our March 2020 report to the Minister we commented on the AFP's practice for extending and varying surveillance device warrants. Specifically, we were of the view that the AFP's use of adhesive labels for extensions and variations of surveillance device warrants was not compliant with the Act because the new expiry date or other varied term was changed on the label rather than on the original warrant.

In response to this finding the AFP advised that it does not consider its approach to extending and varying warrants is non-compliant, but agreed to update its guidance materials to improve the reliability of extensions and variations made using this practice.

At this inspection, which considered records for the period from 1 July to 31 December 2019, we identified a further warrant affected by this issue. In that instance the extension of the warrant was made using an adhesive label. As the eligible Judge or nominated AAT member did not sign or date across the edge of the label and onto the warrant itself, we could not be assured the label was affixed to the original warrant in their presence.

While noting the recurrence of this issue, we consider the AFP's updated guidance material should improve the reliability of this practice and, in turn, mitigate our concerns regarding its compliance with s 19(5) of the Act.

We will continue to monitor the AFP's approach to warrant extensions and variations at future inspections.

Finding—Insufficient information in affidavit

What the Act provides

Under s 14(1) of the Act a law enforcement officer may apply for a surveillance device warrant if they suspect on reasonable grounds that the use of a surveillance device is necessary to enable evidence to be obtained in an investigation into one or more relevant offences.

Under s 14(5)(b) of the Act an application for a surveillance device warrant must be supported by an affidavit setting out the grounds on which the warrant is sought.

Under section 16(1)(a) of the Act, an eligible Judge or nominated AAT member may issue a surveillance device warrant in relation to a relevant offence if satisfied that there are reasonable grounds for the suspicion founding the application for the warrant.

Section 16(2)(c) of the Act states that an eligible Judge or nominated AAT member must have regard to the extent to which the privacy of any person is likely to be affected when determining whether to issue a surveillance device warrant.

The Act does not explicitly require an application for a surveillance device warrant to address privacy. However, in our view the application and supporting affidavit should directly address the matters of which the eligible Judge or nominated AAT member are required to be satisfied when determining the application under s 16 of the Act.

Section 65(1) of the Act provides for minor defects or irregularities in warrants, emergency authorisations and tracking device authorisations to be overcome such that the use of devices and evidence obtained may be used as if the relevant warrant, emergency authorisation or tracking device authorisation did not have a defect or irregularity.

What we found

We identified one instance where the affidavit the AFP used to obtain two warrants did not include privacy considerations. The format of the affidavit appeared to be consistent with other affidavits but, unlike other files we inspected, the paragraphs relating to privacy considerations were not included. We are satisfied this omission was isolated to these particular files and, although we consider the absence of information addressing privacy considerations to be significant, acknowledge that it is not indicative of non-compliance with the Act.

We identified one instance where an affidavit did not include information about an offence which was included on the warrant. In this instance the warrant was issued in respect of two different offences of a similar nature and the affidavit contained information relating to one offence but not the other. While the penalty for both offences met the definition of a relevant offence as required by the Act, it was concerning that not all of the grounds on which the warrant was sought, namely the second offence, were substantiated in the affidavit.

What we suggested

We suggested the AFP seek legal advice regarding the validity of the warrant and any evidence it obtained in relation to the offence that was not mentioned in the relevant affidavit.

We also suggested the AFP review its quality assurance mechanisms to ensure affidavits include all information required in support of applications for surveillance device warrants.

Disclosure—Delay in revocations

What the Act provides

Section 22(1) of the Act provides that a law enforcement officer or another person on his or her behalf, may apply for a retrieval warrant in respect of a surveillance device, installed on a premises or object, under a warrant or authorisation, if they suspect the device is still in or on those premises or object.

Section 27(2) of the Act states that if the chief officer believes the grounds for issuing a warrant no longer exist, the chief officer must by instrument in writing revoke the warrant. Section 27(5) of the Act states that if the law enforcement officer to whom a retrieval warrant has been issued or who is primarily responsible for executing the warrant believes that the grounds for issuing the warrant no longer exist, he or she must inform the chief officer immediately.

What the AFP disclosed

The AFP disclosed an instance where it did not revoke a retrieval warrant in a timely manner after the relevant device was retrieved. In this instance it revoked the retrieval warrant approximately five weeks after it retrieved the relevant device, which we were not satisfied met the requirement under s 27(5) of the Act to act "immediately".

Disclosure—Extra-territorial surveillance

What the Act requires

Under s 42(3) of the Act if, after a surveillance device warrant is issued, it becomes apparent to the law enforcement officer primarily responsible for executing the warrant that there will be a need for surveillance in a foreign country, the warrant is taken to permit that surveillance only if the surveillance has been agreed to by an appropriate consenting official of the foreign country.

What the AFP disclosed

In our March 2020 report to the Minister we reported that the AFP had disclosed an instance where a surveillance device was active while outside of Australia. During this inspection period we inspected a second instance of the same issue, which the AFP had disclosed to us at the same time.[4]

[4] The two instances were inspected separately as they related to different time periods.

In this instance, the relevant warrant did not authorise surveillance outside of Australia. The AFP examined the circumstances surrounding this occurrence and determined that procedural and technical errors had combined to accidently activate the device while it was outside of Australia. The AFP quarantined the files created by the activation, and advised it was investigating more robust methods to prevent devices being accidentally activated.

Finding—Tracking devices retrieved without proper authority

What the Act requires

Section 39(6) of the Act states that, if an authorising officer gives a tracking device authorisation (TDA), the authorising officer may also authorise the retrieval, without a warrant, of the tracking device to which the authorisation relates.

Section 40 of the Act requires that, as soon as practicable after a TDA has been given, the authorising officer must make a record of giving that authorisation including whether the TDA authorises the retrieval of a tracking device. Under s 40(1)(h) of the Act, where the TDA authorises the retrieval of a tracking device, the object or premises from which it is to be retrieved must be specified.

What we identified

We identified three instances where the TDA record did not include wording to specifically authorise the retrieval of the tracking devices. We concluded that the AFP had relied on these TDAs to retrieve the devices, even without this wording, because each occurred while the authorisation was in effect and the AFP did not provide any other records that authorised retrieval.

The absence of clear reference to retrieval in the written record of the TDAs raised questions about whether the tracking devices were retrieved with lawful authority.

The AFP's response

The AFP advised that it had updated its TDA template to include explicit wording to authorise the retrieval of tracking devices at the same time that use and installation of the device is authorised. We will review the updated template at our next inspection.

Finding—Insufficient detail in action sheets

What the Act requires

Section 49 of the Act states that the chief officer must, as soon as practicable after a warrant or authority ceases to be in force, make a report to the Minister. The section outlines what must be included in that report.

Under s 18 of the Act surveillance device warrants permit installation, retrieval and maintenance of devices under the authority of the warrant.

The s 49 report is a key transparency and accountability mechanism that provides visibility to the Minister of the way in which agencies use surveillance devices.

The AFP uses action sheets to document how its staff use surveillance devices. These are required to be completed by investigators and officers installing, retrieving and maintaining a device or 'activating' and 'de-activating' a device. The AFP relies on these action sheets to compile Final Effectiveness Reports, which then inform its reports to the Minister under s 49. We consider action sheets are a key mechanism for the AFP to demonstrate its compliance with the Act when using surveillance devices.

Where action sheets are unclear it is difficult to establish that the information provided in s 49 reports is accurate which, in turn, limits the Office's ability to verify whether actions carried out have been done so under the authority of the relevant warrant or authorisation.

What we found

In four files we inspected, the action sheets did not contain sufficient information about how the AFP executed the warrants and authorisations. This meant that it was not possible for us to assess whether the AFP's actions complied with the requirements of the warrant or authorisation. For example:

- The action sheet for one warrant did not stipulate how the surveillance device was retrieved, or where it was retrieved from.
- The action sheets for three computer access warrants did not contain sufficient details about the AFP's activities under the warrant. In some instances it was not clear whether actions were undertaken remotely.
- It was not clear from the action sheet for one warrant whether a device the AFP installed under the warrant had been retrieved. While the action sheet contained an installation date, there was no corresponding retrieval date.
- The action sheet for one warrant referred to multiple device reference numbers. When asked, the AFP advised that the various reference numbers corresponded

to maintenance of the installed devices but this was not clear on the face of the records.

The AFP advised that, depending on the type of device used, some of the detail required by the action sheet template may not be applicable. In these instances we consider the action sheet should be completed in a way that makes it clear where and why particular information cannot be supplied.

Across the records we inspected, the Office observed that the AFP staff completing action sheets did not consistently follow the guidance contained within those forms. In a number of instances, if officers had followed the AFP's internal guidance they would have been prompted to include sufficient detail to aid our assessment.

The examples above highlight how the lack of specificity within action sheets can create uncertainty about what actions have been taken under a warrant or authorisation. This ambiguity can impact the Office's ability to assess the compliance of reports made under s 49 of the Act and provide assurance to the Parliament and the public that the AFP is using surveillance devices within the authority of the relevant warrant or authorisation.

What we suggested

We suggested the AFP remind its officers of the importance of including appropriate detail in action sheets, particularly in relation to computer access warrants.

The AFP's response

In response to this finding the AFP invited our staff to meet with the team responsible for completing action sheets to discuss our observations and provide feedback about the areas in which we consider greater detail is required. The AFP also:

- amended its action sheet template to encourage staff to include greater detail
- updated its surveillance device training to include the obligations and expectations for action sheets, and
- created a fact sheet and distributed it to all regions to ensure consistency with record keeping requirements.

We will assess these measures at our next inspection.

Disclosure—Original documents not kept

What the Act requires

Section 51(d) of the Act requires the chief officer of a law enforcement agency to ensure each record made under s 40 of the Act in relation to a tracking device authorisation (TDA) is kept. The Office's long standing position is that this requirement relates to original records rather than copies. Consistent with this, the AFP's usual practice is to retain original TDAs.

What the AFP disclosed

The AFP disclosed to us that it had destroyed four original TDAs after they were recorded electronically. Two files included a statutory declaration to the effect that the original TDAs were destroyed because the officer was not aware of the obligation to retain the original.

Our view on this matter

We consider that the original record of a TDA should be retained to meet the requirements of s 51(d) of the Act. We were satisfied that the AFP's usual practice is to retain original TDAs and that the instances of non-compliance above were isolated to one operation and did not appear to reflect a systemic issue. We consider that the record on file to capture what had occurred, along with the disclosure to our Office, was an appropriate response to the identified issue.

Finding—Register does not contain required information relating to control orders

What the Act requires

Under s 53 of the Act, the chief officer of a law enforcement agency must cause a register of warrants, emergency authorisations and tracking device authorisations sought by law enforcement officers of that agency to be kept.

Sections 53(2) to (4) of the Act specify the information to be kept in the register. Under ss 53(2)(c)(iiic) and (iiid) of the Act, where a warrant is issued on the basis of a control order, the register must contain the date the control order was made.

What we identified

During the inspection we reviewed the AFP's surveillance device register to assess its accuracy and completeness. We identified that the register did not contain a mechanism to capture the required detail for a control order, specifically the date the control order was made.

The AFP's response

At the meeting to discuss our findings at the end of our inspection, the AFP advised that it had updated the register to capture the information required by ss 53(2)(c)(iiic) and (iiid) of the Act and had also back-captured the required information for relevant records. We will review these updates at our next inspection.

Finding—Reports not made to the Minister in accordance with the Act

What the Act requires

Section 49 of the Act requires that the chief officer of a law enforcement agency must, as soon as practicable after a warrant, emergency authorisation or tracking device authorisation ceases to be in force, make a report to the Minister and provide copies of the warrant and other specified documents. The Act does not define 'as soon as practicable', but we consider a period of up to three months is generally reasonable.

The reports must include, among other things, the details of any premises on which the device was installed or any place at which the device was used (s 49(2)(b)(vii) of the Act). Under s 6 of the Act premises is defined as: land, a building or vehicle, part of a building or vehicle and any place, whether built on or not; whether within or beyond Australia.

What we found

We identified three instances where the AFP submitted reports more than three months after the warrant or authorisation ceased to be in effect. In one of these instances, the warrant was revoked in August 2019 but the AFP had still not made a report by the time of our inspection in March 2020.

We also identified three instances of incorrect information in s 49 reports:

- One instance where the report incorrectly referred to a vehicle as an object (s 49(2)(b)(vii)) when it should have been recorded as a premises (s 49(2)(b)(vii) of the Act).
- One report did not address how conditions were adhered to. While there were no conditions, this should have been included under s 49(2B)(b)(xi).
- One report stated 'vicinity of [suburb]' as a premises at which the computer was located. However, a general vicinity does not meet the definition of a premises under s 6 of the Act (s 49(2B)(b)(v)).

What we suggested

We suggested the AFP provide amended s 49 reports to the Minister.

Appendix A—Inspection criteria and methodology

Objective: To determine the extent of compliance with the *Surveillance Devices Act 2004* by the agency and its law enforcement officers (s 55).

1. Were surveillance devices used in accordance with the Act?

1.1 Did the agency have the proper authority for the use and/or retrieval of the device?

1.1.1 What are the agency's procedures to ensure that surveillance device warrants, retrieval warrants, revocation warrants and authorisations, are properly applied for and are they sufficient?*	1.1.2 Were authorisations properly granted?*	1.1.3 What are the agency's procedures for seeking extensions and variations, and are they sufficient?*
1.1.4 What are the agency's procedures for revoking surveillance device and retrieval warrants, and are they sufficient?*		

1.2 Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?

1.2.1 What are the agency's procedures to ensure the lawful use of surveillance devices, and are they sufficient?*	1.2.2 Does the agency have an auditable system for maintaining surveillance devices?	1.2.3 What are the agency's systems and /or records capturing the use of surveillance devices, and are they sufficient?*
1.2.4 What are the agency's procedures for ensuring warrant conditions are adhered to, and are they sufficient?*		

2. Were computer access activities conducted in accordance with the Act?

2.1 Did the agency have the proper authority for the doing of certain things in relation to computer access?

2.1.1 What are the agency's procedures to ensure computer access warrants are properly applied for, and are they sufficient?*	2.1.2 What are the agency's procedures for seeking extensions and variations to computer access warrants, and are they sufficient?*	2.1.3 What are the agency's procedures for ensuring discontinuance of access under a computer access warrant, and are they sufficient?*
2.1.4 What are the agency's procedures for revoking computer access warrants, and are they sufficient?*		

2.2 Were computer access activities conducted in accordance with the authority of warrants?

2.2.1 What are the agency's procedures to ensure the lawful doing of things under a computer access warrant, and are they sufficient?*	2.2.2 What are the agency's systems and/or records capturing the things done under a computer access warrant, and are they sufficient?*
2.2.3 What are the agency's procedures for ensuring computer access warrant conditions are adhered to, and are they sufficient?*	

2.3 Did the agency notify the Ombudsman of relevant computer access activities in accordance with the Act?

2.3.1 Did the chief officer of the relevant law enforcement agency notify the Ombudsman in relation to concealment of access activities under a computer access warrant, where those activities took place more than 28 days after the warrant ceased to be in force, and in accordance with the Act?

3. Is protected information properly managed?

3.1 Is protected information properly stored, used and disclosed?

3.1.1 What are the agency's procedures for ensuring the secure storage of protected information, and are they sufficient?*	3.1.2 What are the agency's procedures for ensuring the proper use and disclosure of information, and are they sufficient?*
3.1.3 What are the agency's procedures for ensuring the protection of privacy?	

3.2 Was protected information properly destroyed and/or retained?

3.2.1 What are the agency's procedures for ensuring that protected information is destroyed in accordance with the Act, and are they sufficient?*	3.2.2 What are the agency's procedures for ensuring that protected information is retained in accordance with the Act, and are they sufficient?*
3.2.3 Does the agency regularly review its protected information to ensure compliance with the Act?	

4. Was the agency transparent and were reports properly made?

4.1 Were all records kept in accordance with the Act?

4.1.1 What are the agency's record keeping procedures, and are they sufficient?*

4.2 Were reports properly made?

4.2.1 What are the agency's procedures for ensuring that it accurately reports to the Minister (Department of Home Affairs) and the Commonwealth Ombudsman, and are they sufficient?*

4.3 Was the agency cooperative and frank?

Considerations may include:

1. Does the agency have a culture of compliance?
2. Was the agency proactive in identifying compliance issues?
3. Did the agency disclose issues before or during an inspection?
4. Were issues identified at previous inspection/s addressed by the agency?
5. Has the agency engaged with the Commonwealth Ombudsman's office, as necessary?

* Sufficiency will be tested through secondary checks such as corroborating records.