COMMONWEALTH OMBUDSMAN

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

For the period 1 January to 30 June 2018

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 January to 30 June 2017 and
1 July to 31 December 2017

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 January to 30 June 2017 and
1 July to 31 December 2017

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2017 and
1 July to 31 December 2017

NEW SOUTH WALES POLICE FORCE
Records from 1 July 2016 to 30 June 2017

SOUTH AUSTRALIA POLICE
Records from 1 July 2016 to 30 June 2017

VICTORIA POLICE
Records from 1 July 2016 to 30 June 2017

WESTERN AUSTRALIA POLICE
Records from 1 July 2016 to 30 June 2017

Report by the Commonwealth Ombudsman
under s 61 of the *Surveillance Devices Act 2004*

September 2018

COMMONWEALTH OMBUDSMAN

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

For the period 1 January to 30 June 2018

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 January to 30 June 2017 and
1 July to 31 December 2017

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 January to 30 June 2017 and
1 July to 31 December 2017

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2017 and
1 July to 31 December 2017

NEW SOUTH WALES POLICE FORCE
Records from 1 July 2016 to 30 June 2017

SOUTH AUSTRALIA POLICE
Records from 1 July 2016 to 30 June 2017

VICTORIA POLICE
Records from 1 July 2016 to 30 June 2017

WESTERN AUSTRALIA POLICE
Records from 1 July 2016 to 30 June 2017

Report by the Commonwealth Ombudsman
under s 61 of the *Surveillance Devices Act 2004*

September 2018

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
Level 5, 14 Childers Street
Canberra ACT 2600
Tel: **1300 362 072**
Email: **ombudsman@ombudsman.gov.au**

CONTENTS

OVERVIEW

This report presents the results of inspections conducted by the Commonwealth Ombudsman (the Ombudsman) under s 55 of the *Surveillance Devices Act 2004* (the Act), which were finalised between 1 January and 30 June 2018, for the following agencies:

- Australian Commission for Law Enforcement Integrity
- Australian Criminal Intelligence Commission
- Australian Federal Police
- New South Wales Police Force
- South Australia Police
- Victoria Police
- Western Australia Police

Under the Act, specified law enforcement agencies can covertly use surveillance devices when investigating certain offences. This covert power is given to federal agencies for the purposes of combating crime and protecting the community. The Act also allows certain State and Territory law enforcement agencies to use surveillance devices in relation to the investigation of certain Commonwealth offences and the enforcement of Family Court recovery orders.

The Ombudsman provides independent oversight by conducting inspections at each agency that has exercised Commonwealth surveillance device powers during the selected period. At these inspections, we assess whether agencies are compliant with the Act and have processes in place to support compliance. We also consider agencies' transparency and accountability and encourage agencies to disclose issues to our Office. Where we identified issues at previous inspections, we follow-up on the actions taken by agencies to address these issues.

Overall, our inspections found all agencies to be compliant with the requirements of the Act. We identified some exceptions to compliance regarding the retention of protected information and some minor reporting errors by agencies. We commend the remedial actions taken by agencies to address all issues, including those outstanding from previous inspections.

We note the continued transparency and engagement by agencies with our Office, as evidenced by the disclosure of instances of non-compliance. Agencies were cooperative throughout our inspections and provided access to relevant staff and information. It is evident agencies are committed to compliance and are receptive to our findings and suggestions.

INTRODUCTION

The Act regulates the use of surveillance devices[1] by law enforcement agencies. The Act allows certain surveillance activities to be conducted covertly under a warrant (issued by an eligible Judge or nominated Administrative Appeals Tribunal member), an internally issued authorisation or without formal authority. The Act imposes requirements for the secure storage and destruction of records, and restricts the use, communication and publication of information obtained through the use of surveillance devices.[2] It also imposes reporting obligations on law enforcement agencies to ensure an appropriate level of transparency regarding agencies' covert surveillance device activities.

What we do

The Ombudsman performs the independent oversight mechanism provided in the Act. The Ombudsman is required to inspect the records of each law enforcement agency to determine the extent of their compliance with the Act and report to the relevant Minister (the Minister for Home Affairs) at six-monthly intervals.[3] For security reasons, we do not inspect records relating to authorities which are still in force.

Why we oversee agencies

The use of surveillance devices is one of the most intrusive covert powers afforded to law enforcement agencies. It is the Ombudsman's role to assess the extent to which agencies are compliant with the Act.

How we oversee agencies

We have developed a set of inspection methodologies we consistently apply across all agencies. These methodologies are based on legislative requirements and best practice standards, ensuring the integrity of each inspection.

We focus our inspections on areas of high risk, taking into consideration the impact of non-compliance, for example unnecessary privacy intrusions.

---

1 Under s 6 of the Act, a 'surveillance device' means a data surveillance device, a listening device, an optical surveillance device or a tracking device—or a device that is a combination of any two or more of these devices.

2 This type of information and records are collectively referred to as 'Protected Information' as defined under s 44 of the Act.

3 On 10 May 2018, amendments were made to the Commonwealth of Australia, Administrative Arrangements Order and the responsibility for the administration of the *Surveillance Devices Act 2004*, was transferred from the Attorney-General to the Minister for Home Affairs.

We assess compliance based on the records made available at the inspection, discussions with relevant agency teams, observing agencies' processes through the information provided and remedial action taken by agencies in response to any identified issues.

To ensure agencies are aware of what we will be assessing, we provide them with a broad outline of our criteria prior to each inspection. This assists agencies to identify the most accurate sources of information to assist us with the inspection and in determining agency compliance.

We encourage agencies to be upfront and voluntarily disclose any instances of non-compliance to our Office, including informing us of any remedial action the agency has taken. We can also rely on coercive powers to obtain any information relevant to our inspection, if required.

At the end of each inspection we provide our preliminary findings to the agency, to facilitate any immediate remedial action required. We may also assist agencies in ensuring compliance through assessing agencies' policies and procedures, communicating 'best practices' to meet compliance and engaging with agencies outside of the formal inspection process.

Our criteria

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

We use the following criteria to assess compliance:

1. Did the agency have the proper authority for the use and/or retrieval of the surveillance device?
2. Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?
3. Was protected information properly stored, used and disclosed?
4. Was protected information properly destroyed and/or retained?
5. Were all records kept in accordance with the Act?
6. Were reports properly made?
7. Was the agency cooperative and frank?

For more information on our inspection criteria and methodology, see **Appendix A.**

How we report to the Minister

To ensure procedural fairness, agencies are given an opportunity to comment on the findings from our inspection. After this process, the inspection results are considered finalised. The findings from these reports are de-sensitised and form the basis of the report to the Minister.

As a result of the above process, there will typically be some delay between the date we conducted the inspection and the finalisation of our six-monthly reports to the Minister.

Included in this report is an overview of our compliance assessment of all agencies, a discussion of each agency's progress in addressing any significant findings from previous inspections and details of any significant or systemic issues.

We may also report on issues other than instances of non-compliance, such as the adequacies of an agency's policies and procedures to ensure compliance with the Act.

This report may not include administrative issues or instances of non-compliance where the consequences are negligible, for example when actions did not result in unnecessary privacy intrusion or were minor human errors.

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

We conducted two inspections of the Australian Commission for Law Enforcement Integrity's (ACLEI) surveillance device records within the reporting period, from 9–10 November 2017 and from 21–22 March 2018, respectively.

We identified two issues in the first inspection, these findings are discussed below. We did not identify any issues in the second inspection. However, we identified two instances in which ACLEI's reports to the Minister under s 49 of the Act contained inaccuracies regarding the kind of surveillance devices used. Following the inspection, ACLEI advised it had amended and provided the Minister with both revised reports.

We appreciate ACLEI's assistance in facilitating these inspections and commend its preparedness, specifically in collating relevant information and documents.

INSPECTION ONE

At the November 2017 inspection, we assessed all 17 surveillance device warrants issued to ACLEI which ceased to be in force during the period.

This inspection assessed ACLEI's records from 1 January to 30 June 2017.

We did not assess any authorisations, destructions or retentions of protected information, as ACLEI advised no authorisations ceased to be in force during the period, nor did it destroy or retain any protected information.

Progress made since the previous inspections

At each inspection, we monitor ACLEI's progress in addressing previous inspection findings. This was not necessary for the November 2017 inspection, as no issues were identified at the previous inspection, which covered records from 1 July to 31 December 2016.

Inspection findings

Two issues were identified at this inspection:

Finding 1—Warrant applications did not address privacy

Finding under criterion 1: Did the agency have the proper authority for the use and/or retrieval of the surveillance device?

What the Act requires

Section 14 of the Act outlines the requirements for applying for a surveillance device warrant. Subsection 14(5)(b) provides that an application must be supported by an affidavit setting out the grounds on which the warrant is sought.

Under s 16 of the Act, in order for a surveillance device warrant to be issued, an eligible Judge or Administrative Appeals Tribunal (AAT) member (the issuing authority) must be satisfied there are reasonable grounds supporting the basis of the warrant application. Under s 16(2)(c), in making this determination, the issuing authority must have regard to the extent to which the privacy of any person is likely to be affected.

What we found and ACLEI's remedial action

We rely on records made available at the inspection, including warrant applications and supporting affidavits, to determine whether the agency has considered privacy implications, including options to minimise any unnecessary privacy intrusion.

In six instances, applications made by ACLEI officers did not address the privacy implications likely to result from the use of surveillance devices. Failing to address privacy implications in warrant applications created a risk that the issuing authority did not have all the relevant information for consideration under s 16(2)(c) of the Act.

However, we also noted instances where ACLEI did comprehensively address privacy considerations and that the above issue did not prevent ACLEI's compliance with s 14 of the Act. We also note that ACLEI's policies and procedures are appropriate to meet compliance with the Act.

We suggested ACLEI officers include information in warrant applications and affidavits to address privacy considerations, particularly where there may be increased or unnecessary privacy intrusion. Following the inspection, ACLEI advised that the Executive Director Operations reminded all Operations Branch staff to address privacy considerations in warrant applications and affidavits.

Finding 2—Surveillance device installed and used at premises not specified on the warrant

Finding under criterion 1: Did the agency have the proper authority for the use and/or retrieval of the surveillance device?

What the Act requires

Under s 18 of the Act a surveillance device warrant may authorise the use of a surveillance device on the specified premises.

Subsection 18(5) provides that a warrant may authorise the interference with the property of a person who is not the subject of the investigation if the eligible Judge or nominated AAT member issuing the warrant (the issuing authority) is satisfied the interference is necessary to give effect to the warrant.

Subsection 37(1)(c) allows the use of an optical surveillance device without a warrant where use of the device does not involve entry onto premises without permission, such as a public premises.

What we identified and ACLEI's remedial action

In one instance, ACLEI installed and used an optical surveillance device in a manner not provided for by the warrant, contrary to s 18 of the Act. ACLEI advised the approach was taken in an effort to overcome difficulties it initially encountered with the installation.

The decision to install the device in a different manner was made at the time of installation. These circumstances had not been anticipated, which meant this information regarding the manner of final installation was not included in the warrant application. This removed the possibility for the issuing authority to give consideration to s 18(5) of the Act.

ACLEI's available records did not indicate it had accessed a remedy provided by s 37 of the Act. Therefore, ACLEI did not have the proper authority to install the device in the manner in which it finally did. We note the installation resulted in ACLEI capturing images of parties who were not subjects of its investigation.

We suggested ACLEI quarantine all protected information obtained from the device from further dissemination. Following the inspection, ACLEI advised it had taken this action.

INSPECTION TWO

At the March 2018 inspection, we assessed all three executed surveillance device warrants issued to ACLEI which ceased to be in force during the period.

This inspection assessed ACLEI's records from 1 July to 31 December 2017.

We did not assess any authorisations, destructions or retentions of protected information, as ACLEI advised no authorisations ceased to be in force during the period, nor did it destroy or retain any protected information.

Progress made since the previous inspections

At each inspection, we monitor ACLEI's progress in addressing previous inspection findings. We identified two issues at the previous inspection, which covered records from 1 January to 30 June 2017, discussed above. We were satisfied with the remedial action taken by ACLEI, to address the previous inspection findings.

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

We conducted two inspections of the Australian Criminal Intelligence Commission's (ACIC) surveillance device records from 11–14 September 2017 and from 9–12 April 2018, respectively.

We identified one issue in the first inspection and four issues in the second inspection, two of which were disclosed by the ACIC. These findings are discussed below.

We would like to acknowledge the ACIC's detailed preparation for both inspections. In addition, our access to its systems allowed us to complete our compliance assessments efficiently and comprehensively. We also appreciate the prompt resolution of issues requiring clarification and the ACIC's responsiveness to our inspection findings.

INSPECTION ONE

At the September 2017 inspection we assessed the following, which had expired or were revoked during the relevant period:

- 41 of the 121 surveillance device warrants issued to the ACIC during the period
- the one retrieval warrant issued to the ACIC during the period
- 4 of the 8 tracking device authorisations given by the ACIC which expired or were revoked during the period

We also assessed the ACIC's destruction of protected information during the period, obtained under 59 warrants.

This inspection assessed the ACIC's records from 1 January to 30 June 2017.

Progress made since the previous inspection

At each inspection, we monitor the ACIC's progress in addressing our previous inspection findings. We identified three issues at the previous inspection, two of which were disclosed by the ACIC, in relation to records from 1 July to 31 December 2016.

At the September 2017 inspection, we were satisfied with the remedial action taken by the ACIC to address all previous inspection findings.

Inspection findings

One issue was identified at this inspection:

Finding 1—Protected information handled contrary to the requirements of s 46

Finding under criterion 4: Was protected information properly destroyed and/or retained?

What the Act requires

Section 44 of the Act outlines the information that is considered to be protected information. For the purpose of our inspection we limit our interpretation of protected information to any information obtained from the use of a surveillance device under a warrant.

Under s 46(1)(b) of the Act, as soon as practicable after a record comprising protected information is created, the chief officer must ensure that the record is destroyed if they are satisfied that the record is no longer required for civil or criminal proceedings. The decision to destroy protected information must be made within five years following its creation.

What we identified and the ACIC's remedial action

At the inspection we identified three instances where protected information was not properly destroyed.

In two of these instances, protected information remained on the ACIC's systems, despite the chief officer's delegate being satisfied that the records were no longer required, under s 46(1)(b) of the Act.

We suggested that the ACIC destroy these records as soon as practicable, pursuant to s 46(1)(b) of the Act. Following the inspection, the ACIC advised that it had destroyed these records.

In the third instance, twenty records containing protected information were possibly destroyed by the ACIC prior to the approval of the chief officer or their delegate, contrary to s 46 of the Act.

Following the inspection, the ACIC advised that the records were destroyed after approval, but the date of destruction had been recorded incorrectly due to a typographical error. The ACIC advised that it had amended its records to reflect the correct date.

INSPECTION TWO

At the April 2018 inspection we assessed the following, which had expired or were revoked during the relevant period:

- 34 of the 133 executed surveillance device warrants issued to the ACIC
- the two retrieval warrants issued to the ACIC
- 11 of the 15 tracking device authorisations given by the ACIC.

We did not assess any destructions or retentions of protected information at this inspection, as the ACIC advised it did not destroy or retain any protected information during the inspection period.

This inspection assessed the ACIC's records from 1 July to 31 December 2017.

Progress made since the previous inspection

At each inspection, we monitor the ACIC's progress in addressing our previous inspection findings. We identified one issue at the previous inspection in September 2017, discussed above. We were satisfied with the remedial action taken by the ACIC to address our inspection finding.

Inspection findings

Four issues were identified, two of which were disclosed by the ACIC:

Finding 1—Surveillance device used on a premises where the target was no longer reasonably believed to be or likely to be, contrary to s 18

Finding under criterion 2: Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?

What the Act requires

A premises warrant:

Under s 18(1)(a) of the Act a surveillance device warrant authorises the use of a surveillance device on specified premises. Subsection 18(2)(a) provides that a premises warrant also authorises the installation, use and maintenance of the device on the specified premises.

For a premises warrant, s 17(1)(b)(vi) of the Act states that the warrant must specify the premises on which the use of the surveillance device is authorised.

A person warrant:

Under s 18(1)(c) of the Act, a surveillance device warrant authorises the use of a surveillance device in respect of the conversations, activities or location of a specified person or a person whose identity is unknown. Subsection 18(2)(c) provides that a person warrant also authorises the installation, use and maintenance of the device on premises where the person is reasonably believed to be or likely to be.

For a person warrant, s 17(1)(b)(viii) of the Act states that the warrant must specify the name of the person (if known) or the fact that the person's identity is unknown.

What we found and suggestions to the agency

A person warrant under s 18(1)(c) of the Act was issued to the ACIC, which specified the name of an alias. Under the authority of the person warrant, the ACIC installed an optical device on a premises where a person of interest, believed to be using the alias specified on the warrant, was reasonably likely to be. Based on available records, the person of interest was arrested. Despite this, the ACIC left the device installed on the premises for another four days until it was retrieved.

At the inspection the ACIC confirmed that, during the additional four days, the device remained in use at the premises and continued to capture protected information. The ACIC advised that, during this period, other persons of interest to the investigation were entering the premises and were believed to also be using the alias specified on the warrant.

The records indicated that the person of interest using the alias specified on the warrant was arrested, meaning the grounds authorising the use of the device under s 18(2)(c) of the Act ceased to exist. The ACIC continued to use the device on premises where the specified person could not reasonably be believed to be, or likely to be, following their arrest, contrary to s 18(2)(c).

Where an agency wishes to use surveillance devices in relation to more than one person, these persons must be specified on the warrant in accordance with s 17(1)(b)(viii) of the Act. On the available records, the ACIC did not appear to have authority under the person warrant for more than one person using the listed alias. It is our position that the person warrant only authorised the use of the device for one person.

We suggested the ACIC seek advice regarding the continued use of the device on the premises, in relation to the additional persons of interest using the alias specified on the warrant. We also suggested the ACIC quarantine from further

dissemination all protected information obtained from the device during the additional four days.

Agency disclosed information and remedial action

Following the inspection, the ACIC advised that in addition to the person warrant, it had obtained a premises warrant under s 18(1)(a) of the Act. The ACIC confirmed that the relevant enforcement officer had sought and been issued both a person and premises warrant.

The ACIC advised that its records did not correctly reflect which warrant it had relied on in this instance. Further, the ACIC disclosed that as a result of incorrect records, it was not compliant with its reporting obligations to the Minister on the execution of these warrants, under s 49 of the Act.

The ACIC confirmed it has amended all applicable records relating to the authority to install and use a surveillance device under the premises warrant. The ACIC advised it had drafted and will provide an amended s 49 report for the Minister, in relation to the executed premises warrant.

We appreciate the clarification and additional information provided by the ACIC. However, until we are able to review the ACIC's records at the next inspection, we cannot confirm compliance with the Act.

Finding 2—Agency disclosed written permission for tracking device authorisations not given in accordance with s 39

Finding under criterion 1: Did the agency have the proper authority for the use and/or retrieval of the surveillance device?

What the Act requires

Section 39 of the Act provides for the use of a tracking device without a warrant, defined as a tracking device authorisation under s 6 of the Act. Subsection 39(1) of the Act states that a law enforcement officer may, with the written permission from an appropriate authorising officer, use a tracking device without a warrant in the investigation of a relevant offence. The authorisation must indicate the period the authorisation remains in force, not exceeding 90 days, under s 39(7) of the Act.

Under s 39(9), the law enforcement officer must apply for the tracking device authorisation orally or in writing and address the same matters required as if they were making an application for a surveillance device warrant under the Act. Section 40 states the appropriate authorising officer must make a written record

as soon as practicable after they have given the tracking device authorisation, including what that record must include.

Agency disclosed non-compliance and remedial action

Prior to our inspection, the ACIC disclosed four instances where appropriate authorising officers either did not provide their permission in writing when giving a tracking device authorisation, or written permission was provided but did not indicate the period for which the authorisation was to remain in force, contrary to s 39 of the Act.

Upon identifying the non-compliance, the ACIC implemented a number of remedial measures, such as briefing relevant staff on the requirements when applying for tracking device authorisations, and updated its procedures. As an additional measure, where the tracking device authorisation was executed, the ACIC quarantined any protected information obtained.

What we found

At the inspection, we sighted evidence of the ACIC's remedial action and confirmed that all protected information obtained by devices used under these authorisations was quarantined. Despite these instances of non-compliance, we note the detailed nature of the ACIC's records, particularly in circumstances where tracking device authorisations are applied for orally.

Finding 3—Retrieval warrant not revoked after device retrieved, contrary to s 27

Finding under criterion 2: Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?

What the Act requires

Subsection 27(2) states that if the chief officer is satisfied that the grounds for issue of the retrieval warrant no longer exist, the chief officer must, by instrument in writing, revoke the warrant.

Subsection 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 issue of the warrant no longer exist, he or she must inform the chief officer immediately.

Subsection 22(1) provides for a law enforcement officer (or another person on his or her behalf) to 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 on those premises or object.

What we identified and the ACIC's remedial action

We found one instance where the ACIC retrieved a surveillance device under a retrieval warrant, and left the warrant to expire five days later. The retrieval of the device occurred late on a Thursday afternoon and the warrant expired the following Tuesday. We acknowledge that due to a weekend, there may have been limited opportunity to allow for, or request, the revocation of the retrieval warrant by the chief officer.

In this instance, the ACIC did not appear to be compliant with the requirements under ss 27(2) or 27(5) of the Act. Based on the records available at our inspection, there was no information to indicate why the retrieval warrant was not revoked, or whether the chief officer was immediately informed once the grounds for issue of the warrant ceased to exist. Our Office interprets the reference to 'immediately' in s 27(5) as meaning the same day or as soon as possible on the following business day.

We note the ACIC's current draft Surveillance Devices Procedure states retrieval warrants must be revoked upon device retrieval. We noted in another instance the ACIC had recorded a detailed explanation outlining why an investigator did not immediately seek revocation of a retrieval warrant, upon the successful retrieval of the device. Maintaining records such as this provides our Office with a higher level of confidence that the ACIC is aware of its revocation obligations under s 27 of the Act.

Following the inspection, the ACIC advised it has included a reminder within both of its fortnightly advice and reminder emails to staff, reiterating its revocation obligations under s 27 of the Act.

Finding 4—Agency disclosed protected information handled contrary to the requirements of s 46

Finding under criterion 4: Was protected information properly destroyed and/or retained?

What the Act requires

Section 44 of the Act outlines the information that is considered to be protected information. For the purpose of our inspection we limit our interpretation of

protected information to any information obtained from the use of a surveillance device under a warrant.

Under s 46(1)(b) of the Act, as soon as practicable after a record or report, comprising protected information is created, the chief officer must ensure that the record is destroyed, if they are satisfied that the record is no longer required for civil or criminal proceedings. The decision to destroy protected information must be made within five years following its creation. The chief officer may decide to retain protected information, however this decision must be recorded. If the chief officer decides to retain protected information, the decision must be made every five years until its destruction.

Subsection 46(3) provides an exception for protected information received into evidence in legal or disciplinary proceedings.

Agency disclosed non-compliance and remedial action

The ACIC disclosed three separate instances of handling protected information contrary to its requirements under the Act.

In the first instance, the ACIC was unable to locate protected information obtained from the use of a device. It was therefore unable to confirm the destruction of this information, despite the chief officer's delegate being satisfied that the record was no longer required, under s 46(1)(b) of the Act.

In the second instance, protected information held by a partner agency of the ACIC was unable to be destroyed (due to system limitations at that agency), despite the chief officer's delegate being satisfied that the record was no longer required, under s 46(1)(b) of the Act. We note the ACIC's efforts to seek confirmation from the partner agency as to the status of the protected information.

In the third instance, protected information held on the ACIC's system was destroyed two days after the five year period within which the information had to be actioned, in accordance with s 46(1)(b)(ii) of the Act.

Despite these instances of non-compliance, we are satisfied the ACIC has adequate destruction procedures in place and understands its obligations in order to be compliant with the Act.

AUSTRALIAN FEDERAL POLICE

We conducted two inspections of the Australian Federal Police's (AFP) surveillance device records on 4–7 September 2017 and 27 February to 2 March 2018, respectively.

We identified two issues at our first inspection, one of which was disclosed by the AFP. We identified three issues at our second inspection, one of which was disclosed by the AFP, these findings are discussed below.

We commend the AFP's continued transparency in disclosing instances of non-compliance to our Office. We would like to acknowledge the AFP's cooperation during both inspections and its responsiveness to our inspection findings.

INSPECTION ONE

At the September 2017 inspection we assessed the following, which had expired or were revoked during the relevant period:

- 54 of the 413 surveillance device warrants issued to the AFP
- 6 of the 25 retrieval warrants issued to the AFP
- 4 of the 12 tracking device authorisations given by the AFP.

We also assessed the AFP's destruction and retention of protected information obtained under warrants. We assessed 62 of the 179 destructions and 32 of the 57 retentions during the inspection period.

This inspection assessed the AFP's records from 1 January to 30 June 2017.

Progress made since the previous inspection

At each inspection, we monitor the AFP's progress in addressing previous inspection findings. The previous inspection period covered records from 1 July to 31 December 2016.

We identified three issues at the previous inspection, one of which was disclosed by the AFP. The most significant of these issues related to non-compliance with the destruction and retention provisions of the Act. Overall, we were satisfied with the remedial action taken by the AFP to address all previous inspection findings.

Inspection findings

Two issues were identified, one of which was disclosed by the AFP:

Finding 1—Agency disclosed surveillance device remained activated after the warrant expired, contrary to s 18 and after authorisation expiry, contrary to s 39

Finding under criterion 2: Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?

What the Act requires

Subsection 18(1) of the Act provides that a surveillance device warrant authorises the use of a surveillance device on specified premises, specified objects or class of object or for a specified person or a person whose identity is unknown, respectively. Subsection 18(2) further provides that a surveillance device warrant will authorise the installation, use, maintenance and retrieval of that device.

Section 39 of the Act provides for the use of a tracking device without a warrant, defined as a tracking device authorisation under s 6 of the Act.

Agency disclosed non-compliance and remedial action

The AFP disclosed two instances where surveillance devices were left activated on specific premises after the expiration of the warrants.

The AFP was issued with two surveillance device warrants in relation to the same investigation, authorising the use of devices in respect of a specified premises. According to the available records, the devices were already installed on the premises under previous warrants and were reactivated under these warrants. The warrants were not extended and expired. In relation to both warrants, the devices were left activated until they were deactivated by a partner agency a day later.

The AFP advised the first device had already stopped capturing protected information by the deactivation date. For the second device, the AFP advised protected information was captured on the device between warrant expiry and deactivation. Following the inspection, the AFP advised the protected information obtained under the second device was quarantined from further use.

The AFP also disclosed one instance where tracking devices were left activated without lawful authority. The AFP issued a tracking device authorisation and subsequently installed two tracking devices. The authorisation expired, but the devices were not deactivated by the AFP until approximately one month later.

Following the inspection, the AFP advised this oversight occurred due to the responsible officer being on leave at the time the authorisation expired. The AFP advised it provided internal training to the relevant team to reinforce its obligations under the Act.

Finding 2—Protected information handled contrary to the requirements of s 46

Finding under criterion 4: Was protected information properly destroyed and/or retained?

What the Act requires

Section 44 of the Act outlines the information that is considered to be protected information. For the purpose of our inspection, we limit our interpretation of protected information to any information obtained from the use of a surveillance device under a warrant.

Under s 46(1)(b) of the Act, as soon as practicable after a record or report, comprising protected information is created, the chief officer must ensure that the record is destroyed if they are satisfied that the record is no longer required for civil or criminal proceedings. The decision to destroy protected information must be made within five years following its creation. The chief officer may decide to retain protected information, however this decision must be recorded. If the chief officer decides to retain protected information, the decision must be made every five years until its destruction.

Subsection 46(3) provides an exception for protected information received into evidence in legal or disciplinary proceedings.

What we identified and the AFP's remedial action

We identified five instances in which protected information was destroyed or retained by the AFP, contrary to s 46(1)(b) of the Act.

In two instances, protected information was destroyed by the AFP one month after the five year period within which the chief officer (or delegate) should have determined whether to retain or destroy this information under s 46(1)(b)(ii) of the Act. Following the inspection the AFP advised this information had been destroyed, in accordance with the Act.

In two instances, protected information was retained by the AFP without the chief officer's (or delegate's) approval, as required under s 46(1)(b) of the Act. In both instances, the five year period for review by the chief officer (or delegate), to destroy or retain the information was required by October or November 2012,

respectively. However, on the available records, the delegate's approval to retain these records was given in May 2014. The AFP advised this error occurred due to not having auditing procedures in place during 2012, which was rectified in 2016 by including auditing steps in the destruction process. We note these records were subsequently destroyed during this inspection period, which was why the issue was identified and assessed at this inspection.

In one instance, protected information was still located on the AFP's systems at the time of our inspection, despite the chief officer's delegate being satisfied that the records were no longer required, under s 46(1)(b) of the Act. We suggested the AFP destroy this information as soon as practicable. Following the inspection, the AFP advised this information had been destroyed in accordance with the Act.

INSPECTION TWO

At the February/March inspection we assessed the following, which had expired or were revoked during the relevant period:

- 51 of the 303 executed surveillance device warrants issued to the AFP
- 6 of the 9 retrieval warrants issued to the AFP
- 7 of the 21 tracking device authorisations given by the AFP.

We also assessed the AFP's destruction and retention of protected information obtained under warrants. We assessed 51 of the 388 destructions and all eight of the retentions during the inspection period.

This inspection assessed the AFP's records from 1 July to 31 December 2017.

Progress made since the previous inspection

At each inspection, we monitor the AFP's progress in addressing the previous inspection findings. There were two issues at the previous inspection, covering records from 1 January to 30 June 2017, which are discussed above. We were satisfied with the remedial action taken by the AFP to address all previous inspection findings.

Inspection findings

Three issues were identified, one of which was disclosed by the AFP:

Finding 1—Agency disclosed protected information was captured without lawful authority

Finding under criterion 2: Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?

What the Act requires

Under s 18(1)(c) of the Act a surveillance device warrant authorises the use of a surveillance device in respect of the conversations, activities or location of a specified person or a person whose identity is unknown.

Under s 19(1) of the Act a law enforcement officer to whom a surveillance device warrant has been issued (or another person on his or her behalf) may apply, at any time before the expiry of the warrant, for an extension or variation of a warrant.

An application for an extension or variation of the warrant is to be made to an eligible Judge or to a nominated AAT member (the issuing authority), under s 19(2) of the Act. An application for an extension can be made more than once, under s 19(6) of the Act.

Agency disclosed non-compliance and remedial action

The AFP disclosed one instance where surveillance devices continued to capture protected information without lawful authority.

The AFP was issued with a surveillance device warrant which authorised the use of devices in respect of the conversations, activities or location of a specified person, under s 18(1)(c) of the Act. The AFP installed devices under the authority of that person warrant.

The warrant was extended three times and expired at approximately midnight. Following expiration, the AFP was issued with a new warrant the following morning at approximately 9:15am. During the period between the original warrant's expiry and the issuing of the new warrant, the AFP continued to capture protected information on the installed devices without lawful authority.

Upon identifying this issue, the AFP advised it quarantined the protected information captured during the overnight period, noting that, despite remaining

activated during the period, the devices did not capture any conversations, activities or locations of the person of interest or other persons.

The AFP advised that the week prior to the warrant's expiry, it had attempted to obtain another extension for this warrant, but no AAT member was available. The AFP also advised that, due to the type of devices installed, it could not deactivate the devices, and it was not possible for the devices to be retrieved.

We note the AFP's attempts to obtain an extension on this warrant and that the AFP quarantined the protected information that was captured without lawful authority.

Finding 2—Retrieval warrants not revoked after devices retrieved

Finding under criterion 2: Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?

What the Act requires

Subsection 27(2) states that if the chief officer is satisfied that the grounds for issue of the retrieval warrant no longer exist, the chief officer must, by instrument in writing, revoke the warrant.

Subsection 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 issue of the warrant no longer exist, he or she must inform the chief officer immediately.

Subsection 22(1) provides for a law enforcement officer (or another person on his or her behalf) to 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 on those premises or object.

What we identified and the AFP's remedial action

We identified three instances where retrieval warrants were not revoked by the AFP, despite the respective devices being retrieved.

In the first instance, the device was retrieved and the retrieval warrant was left to expire three months later. In the second instance, the device was retrieved and the retrieval warrant was left to expire eight days later. In the third instance, a device was retrieved but the retrieval warrant was not revoked for another twelve days.

According to the available records, there was no indication whether the chief officer was immediately informed once the grounds for issue of the retrieval warrants ceased to exist, as required under s 27(5) of the Act. Our Office interprets the reference to 'immediately' as being the same day or as soon as possible on the following work day.

We note the AFP's National Guideline for Surveillance Devices states retrieval warrants must be revoked upon device retrieval. At the inspection, there appeared to be inconsistency in the AFP's application of this process. In some instances, retrieval warrants were revoked immediately after device retrieval and in others, as detailed above, they were not. This may suggest a knowledge gap whereby some investigators are unaware of their revocation obligations under s 27 of the Act.

Following the inspection, the AFP advised it has introduced retrieval surveillance device action sheet checks for the relevant teams. The AFP expressed its commitment to ongoing education for staff on its obligations under the Act.

Finding 3—Protected information handled contrary to s 46 requirements

Finding under criterion 4: Was protected information properly destroyed and/or retained?

What the Act requires

Section 44 of the Act outlines the information that is considered to be protected information. For the purpose of our inspection we limit our interpretation of protected information to any information obtained from the use of a surveillance device under a warrant.

Under s 46(1)(b) of the Act, as soon as practicable after a record comprising protected information is created, the chief officer must ensure that the record is destroyed, if they are satisfied that the record is no longer required for civil or criminal proceedings. The decision to destroy protected information must be made within five years following its creation. The chief officer may decide to retain protected information, however this decision must be recorded. If the chief officer decides to retain protected information, the decision must be made every five years until its destruction.

Subsection 46(3) provides an exception for protected information received into evidence in legal or disciplinary proceedings.

What we found and the AFP's remedial action

We identified one instance, and the AFP disclosed one instance, where protected information was not destroyed in accordance with the Act.

The AFP disclosed one instance where the decision to destroy protected information was made by the chief officer's delegate one month after the five year period in which action on the protected information was required under s 46(1)(b)(ii) of the Act. The AFP advised this oversight occurred due to the incorrect date being entered into the database it uses to track the five year legislative timeframe.

We identified one instance where protected information, consisting of seven electronic files, was still located on the AFP's systems, despite the chief officer's delegate being satisfied that the records were no longer required under s 46(1)(b) of the Act. We suggested the AFP destroy this information as soon as practicable. Following the inspection, the AFP advised these records had been destroyed in accordance with the Act.

We also identified one instance where it appeared protected information was destroyed by the AFP prior to the approval of the chief officer's delegate. Upon further review, we are satisfied this was an administrative (typographical) error, rather than protected information being destroyed without the chief officer's (or delegate) approval.

NEW SOUTH WALES POLICE FORCE

We conducted an inspection of the New South Wales Police Force's (NSWPF) surveillance device records on 23–24 November 2017. We identified one issue, including making one suggestion to the NSWPF, and the NSWPF made one disclosure—these are discussed below.

We would like to acknowledge the NSWPF's cooperation during this inspection and its responsiveness to our inspection findings.

Inspection details

At this inspection, we assessed all five surveillance device warrants issued to the NSWPF, which expired or were revoked during the inspection period.

This inspection assessed the NSWPF's records from 1 July 2016 to 30 June 2017.

Progress made since the previous inspection

At each inspection, we monitor the NSWPF's progress in addressing previous inspection findings. We identified two issues at the previous inspection, which covered records from 1 July 2015 to 30 June 2016.

We were satisfied with the remedial action taken by the NSWPF to address all previous inspection findings.

Inspection findings

One issue and one suggestion identified at this inspection:

Finding 1—Report error under s 50 and non-compliance with reporting requirement under s 49

Finding under criterion 6: Were reports properly made?

What the Act requires

Section 49 of the Act outlines the reporting requirements for each warrant issued to, and authorisation given by, an agency. This section states the chief officer must, as soon as practicable after a warrant ceases to be in force, provide the Minister with a report, a copy of the warrant and other specified documents. Where a warrant or authorisation is executed, the agency is required to provide additional details in the report to the Minister. This reporting obligation includes non-executed warrants.

The term 'as soon as practicable' is not defined in the Act. To ensure consistency and fairness in our approach, we take this to mean a maximum of three months after the warrant or authorisation is revoked or expires.

Under s 50(1) of the Act, the chief officer must submit to the Minister, as soon as practicable after the end of each financial year, a report outlining the agency's use of the surveillance devices powers during that financial year. Subsection 50(1)(a) specifically requires the agency to report the number of applications for warrants made by, or on behalf of, and the number of warrants issued to the agency.

The reporting obligations in the Act are an important transparency and accountability mechanism regarding an agency's covert surveillance device activities.

What we found

During the inspection, we identified one instance where a record, reported by the NSWPF to the Minister as a single warrant, consisted of two separate warrants.

The first warrant was issued to the NSWPF and, upon issue, a number of errors with the warrant were identified. As a result, the warrant was subsequently revoked by the issuing authority and a new warrant was issued two hours later on the same day. Both warrants were based on the same application and supporting affidavit.

Based on the records made available at the inspection, it is our assessment the NSWPF was issued with two separate warrants—the first being the erroneous warrant which was revoked and the second being the new warrant subsequently executed by the NSWPF. As the NSWPF recorded this as one warrant, it has misreported to the Minister the number of warrants it was issued during the 2016–17 financial year, contrary to s 50(1)(a) of the Act.

We also note it appeared the NSWPF only submitted a report to the Minister in relation to the second warrant, under s 49 of the Act.

We suggest, if it has not already done so, the NSWPF notify the Minister of the misreporting of its warrant statistics under the s 50 report and submit a s 49 report as soon as practicable regarding the erroneous warrant.

Disclosed issue and remedial action

The NSWPF also disclosed four instances where it provided s 49 reports to the Minister more than three months after the respective warrants had expired or were revoked. The delay in reporting varied from five to fifteen months. The NSWPF advised it was in the process of finalising procedures to provide guidance to staff on its reporting requirements. NSWPF also advised this would be supplemented by staff training.

Due to the retrospective nature of our inspections, the effectiveness of the NSWPF's remedial action will not be evident until the next inspection.

Finding 2—Suggestion regarding the destruction or retention of protected information

Suggestion made with consideration to criterion 4: Was protected information properly destroyed and/or retained?

What the Act requires

Section 44 of the Act outlines the information that is considered to be protected information. For the purpose of our inspection we limit our interpretation of protected information to any information obtained from the use of a surveillance device under a warrant.

Under s 46(1)(b) of the Act, as soon as practicable after a record or report, comprising protected information is created, the chief officer must ensure that the record is destroyed, if they are satisfied that the record is no longer required for civil or criminal proceedings. The decision to destroy protected information must be made within five years following its creation. The chief officer may decide

to retain protected information, however this decision must be recorded. If the chief officer decides to retain protected information, the decision must be made every five years until its destruction.

Subsection 46(3) provides an exception to ss 46(1) and 46(2) if protected information is received into evidence in legal or disciplinary proceedings.

What we found

The NSWPF has a framework in place for regular reviews of protected information obtained under every warrant and authorisation, which was implemented in response to a recommendation we made in March 2012. This framework requires investigators to complete a memorandum indicating whether records consisting of protected information should be retained or destroyed.

During the inspection, we identified three instances where completed memorandums indicated the investigator was satisfied the protected information should be retained or destroyed. Despite this, the NSWPF had not taken any subsequent action to manage the protected information accordingly. As it had not been five years since the creation of the protected information, nor had the chief officer been made aware of the status of the protected information, the inaction by NSWPF did not result in non-compliance.

What we suggested

We suggest the NSWPF strengthen its destruction and retention process by ensuring follow up action is taken once investigators complete the memorandum, including seeking the approval of the chief officer to retain or destroy the protected information. This will ensure the NSWPF is not keeping records it has indicated it no longer requires, which could result in unnecessary privacy intrusion.

SOUTH AUSTRALIA POLICE

We conducted an inspection of South Australia (SA) Police's surveillance device records on 29 May to 1 June 2018. We identified one issue during this inspection, in relation to the destruction or retention of protected information—this finding is discussed below.

We would like to acknowledge SA Police's cooperation during this inspection and its responsiveness to our inspection finding.

Inspection details

At this inspection, we assessed both of the two surveillance device warrants issued to SA Police, which expired or were revoked during the inspection period.

This inspection assessed SA Police's records from 1 July 2016 to 30 June 2017.

Progress made since the previous inspection

At each inspection, we monitor SA Police's progress in addressing previous inspection findings. The previous inspection was in August 2014 and covered records from 1 July 2012 to 30 June 2013.[4] At that inspection we identified three issues in relation to SA Police's records management, including the use and communication of protected information.

At our recent inspection, we conducted a number of process checks with SA Police regarding its reporting and record keeping procedures for surveillance devices. We are satisfied SA Police has taken adequate remedial action to address all previous inspection findings.

SA Police only made one application for, and was issued one surveillance device warrant for, the reporting period 1 July 2015 to 30 June 2016. We did not conduct an inspection for that reporting period, but reviewed SA Police's records in relation to that warrant in our recent inspection.

[4] SA Police did not use the Commonwealth surveillance device powers during the reporting periods 1 July 2013 to 30 June 2014 and 1 July 2014 to 30 June 2015. As a result, we did not conduct an inspection of SA Police records for those reporting periods.

Inspection findings

One issue was identified at this inspection:

Finding 1—Protected information handled contrary to the requirements of s 46

Finding under criterion 4: Was protected information properly destroyed and/or retained?

What the Act requires

Section 44 of the Act outlines information that is considered to be protected information. For the purpose of our inspection we limit our interpretation of protected information to any information obtained from the use of a surveillance device under a warrant.

Under s 46(1)(b) of the Act, as soon as practicable after a record or report comprising protected information is created, the chief officer must ensure that the record is destroyed, if they are satisfied that the record is no longer required for civil or criminal proceedings. The decision to destroy protected information must be made within five years following its creation. The chief officer may decide to retain protected information, however this decision must be recorded. If the chief officer decides to retain protected information, the decision must be made every five years until its destruction.

What we identified and SA Police's remedial action

For all nine surveillance device warrants issued to SA Police during 2012, there was nothing on the files provided to indicate the chief officer had caused the protected information obtained under these warrants to either be retained or destroyed. These records did not appear to relate to legal or disciplinary proceedings.

As these records were created in 2012, the chief officer was required to make this decision in 2017 to comply with the five year timeframe under s 46(1) of the Act.

We suggested that SA Police action these records as soon as practicable, in accordance with s 46 of the Act. Following the inspection, SA Police advised our Office that the protected information obtained under all nine surveillance device warrants had been destroyed.

VICTORIA POLICE

We conducted an inspection of Victoria Police's surveillance device records on 21–22 August 2017. At this inspection, we identified two issues—these findings are discussed below.

We would like to acknowledge Victoria Police's cooperation during this inspection and its responsiveness to our inspection findings.

Inspection details

At this inspection we assessed the following, which had expired or been revoked during the relevant period:

- all three of the surveillance device warrants issued to the Victoria Police
- the one tracking device authorisation given by the Victoria Police.

We also assessed Victoria Police's destruction of protected information during the period, obtained under eight warrants.

This inspection assessed Victoria Police's records from 1 July 2016 to 30 June 2017.

Progress made since the previous inspection

At each inspection, we monitor Victoria Police's progress in addressing previous inspection findings. Our previous inspection at Victoria Police was conducted in September 2013 and covered records from 1 July 2012 to 30 June 2013. We did not make any suggestions as a result of that inspection.

Victoria Police did not use the Commonwealth surveillance device powers during the reporting periods 1 July 2013 to 30 June 2014, 1 July 2014 to 30 June 2015 or 1 July 2015 to 30 June 2016. As a result, we did not conduct an inspection of Victoria Police's records for those reporting periods.

Inspection findings

Two issues were identified at this inspection:

Finding 1—Protected information handled contrary to the requirements of s 46

Finding under criterion 4: Was protected information properly destroyed and/or retained?

What the Act requires

Section 44 of the Act outlines the information that is considered 'protected information'. For the purpose of our inspection we limit our interpretation of protected information to any information obtained from the use of a surveillance device under a warrant.

Under s 46(1)(b) of the Act, as soon as practicable after a record or report, comprising protected information is created, the chief officer must ensure that the record is destroyed, if they are satisfied that the record is no longer required for civil or criminal proceedings. The decision to destroy protected information must be made within five years following its creation. The chief officer may decide to retain protected information, however this decision must be recorded. If the chief officer decides to retain protected information, a new decision must be made every five years until its destruction.

Subsection 46(3) provides an exception to s 46, in relation to protected information received into evidence in legal or disciplinary proceedings.

What we found

We identified two instances, in the records available at the inspection, where protected information was destroyed prior to the chief officer being satisfied that the records were no longer required. Following the inspection, Victoria Police advised our Office of two additional instances where protected information was destroyed by investigators prior to the chief officer's approval. All of these destructions were conducted prior to the chief officer's approval, contrary to s 46(1)(b) of the Act.

We also note, in the second instance, Victoria Police's records indicated the protected information was destroyed eight to nine months after the information was required to be actioned in accordance with s 46(1)(b)(ii) of the Act. In order for Victoria Police to be compliant with s 46(1)(b)(ii) of the Act, the chief officer needed to certify the protected information for destruction or retention, no later than five years from the date the protected information was created.

At the inspection, we conducted a number of process checks with Victoria Police. As a result, and despite the above issues, we believe Victoria Police has adequate processes in place relating to the retention or destruction of protected information.

Finding 2—Warrants issued for a period of more than 90 days, contrary to s 17(1A)(a)

Finding under criterion 1: Did the agency have the proper authority for the use and/or retrieval of the surveillance device?

What the Act requires

Section 17 of the Act outlines what a surveillance device warrant must specify. Subsection 17(3) of the Act requires that an eligible Judge or nominated AAT member who has determined that a warrant should be issued under the Act must sign the warrant. Once a warrant is signed by the issuing person it is deemed to have been issued; unless another issue date is specified on the warrant under s17(1)(iv) of the Act. Subsection 17(1A)(a) of the Act states that a surveillance device warrant may only be issued for a period of no more than 90 days.

Section 65 of the Act states that information or a record obtained through the use of a surveillance device warrant which contains a defect or irregularity is to be treated as a valid warrant if, not for the defect or irregularity, it would be a sufficient authority for the use of the device to obtain the information or record. Subsection 65(2) states that a defect or irregularity in relation to a warrant under s 65(1) does not include a substantial defect or irregularity.

What we found

We identified two instances where surveillance device warrants issued to Victoria Police were issued for a period of 91 days, contrary to s 17(1A)(a) of the Act. In both instances this error appears to have resulted from Victoria Police miscalculating the 90 days as commencing the day after issue, rather than inclusive of the day of issue. In both instances, the warrants were not executed and were subsequently revoked.

Errors of this type create risk, in circumstances where a warrant is executed, that the additional day may give rise to non-compliance with the Act. We note it is up to agencies to consider whether it is appropriate to rely on s 65 of the Act in relation to this type of error with a surveillance device warrant or other identified defects or irregularities.

WESTERN AUSTRALIA POLICE

We conducted an inspection of the Western Australia Police's (WAPOL) surveillance device records on 6–7 November 2017. We identified one administrative issue and one security suggestion for protected information—these findings are discussed below.

We would like to acknowledge WAPOL's cooperation during this inspection and its responsiveness to our inspection findings.

Inspection details

At this inspection, we assessed all three surveillance device warrants issued to WAPOL, which expired or were revoked during the inspection period.

This inspection assessed WAPOL's records from 1 July 2016 to 30 June 2017.

Progress made since the previous inspection

At each inspection, we monitor WAPOL's progress in addressing the previous inspection findings. We did not identify any issues at the previous inspection, which covered records from 1 July 2015 to 30 June 2016.

At the previous inspection, WAPOL advised it had not destroyed or retained any protected information during the inspection period, therefore this was not assessed during the inspection.

Since our previous inspection, WAPOL implemented a number of actions to strengthen its destruction and retention processes for protected information. These included:

- developing new Standard Operating Procedures
- implementing a new report to outline a recommendation to either destroy or retain the protected information
- establishing a new position for a 'destructions officer' to ensure destructions are completed in accordance with the Act.

Based on these changes, we are satisfied WAPOL has sufficient policies and procedures in place to ensure its destruction and retention of protected information processes are sufficient to achieve compliance with the Act.

Inspection findings

One issue and one suggestion were identified at this inspection:

Finding 1—Administrative error: Warrant application referred to repealed legislation

Finding under criterion 1: Did the agency have the proper authority for the use and/or retrieval of the surveillance device?

What the Act requires

Subsection 14(1)(a) of the Act, states that a law enforcement officer (or another person on his or her behalf), may apply for the issue of a surveillance device warrant if the law enforcement officer suspects on reasonable grounds that one or more relevant offences have been, are being, are about to be, or are likely to be, committed.

The definition of 'relevant offence' under s 6 of the Act, includes an offence against the law of the Commonwealth that is punishable by a maximum term of imprisonment of three years or more, or for life.

What we found

In one instance, a WAPOL officer listed on a warrant application a relevant offence in contravention of legislation that had been repealed prior to the warrant application. The error appeared to result from the officer using a previous warrant application as a template.

A second offence was also listed on the warrant application. Based on the available records, we were able to conclude that WAPOL was investigating relevant offences, for the purpose of s 14(1) of the Act. This meant that despite the above mentioned error, this application did not result in non-compliance, as the 'relevant offence' threshold was established.

This administrative error highlights the need for officers to always use blank templates, rather than rely on previous applications. Revising old applications creates a risk of rewording outdated and inaccurate information, which may result in non-compliance with the requirements of the Act.

Finding 2—Suggestion regarding tracking device authorisations

Suggestion made with consideration to criterion 3: Was protected information properly stored, used and disclosed?

What the Act requires

Section 44 of the Act outlines the information that is considered to be protected information. For the purpose of our inspection we limit our interpretation of protected information to any information obtained from the use of a surveillance device under a warrant.

Section 45 imposes penalties regarding the use, recording, communication or publication of protected information or its admission in evidence except in certain circumstances.

Subsection 46(1)(a) of the Act, requires the chief officer of a law enforcement agency to ensure that every record or report comprising protected information is kept in a secure place that is not accessible to people who are not entitled to deal with the protected information.

What we suggested

During the inspection, we made a suggestion to WAPOL to encrypt the universal serial bus (USB) device it uses to store protected information.

Although we are satisfied that WAPOL has sufficient controls in place to ensure the physical security of the USB device, significant risk arises should the USB device be transferred outside of WAPOL's premises or be misplaced.

APPENDIX A—INSPECTION CRITERIA AND METHODOLOGY

Inspection focus (1): *Were surveillance devices used in accordance with the Act?*		
Relevant Criteria	**Procedural checks**	**Records-based checks**
1. Did the agency have the proper authority for the use and/or retrieval of the surveillance device?	We check the agency has policies and procedures to ensure: • warrants, authorisations, extensions and variations are properly applied for • authorisations are properly granted • extensions and variations are properly sought • warrants are properly revoked.	We inspect applications, warrants, authorisations, variations and other agency records, to assess whether: • applications for surveillance device warrants were made in accordance with s 14 • applications for extensions and/or variations to surveillance device warrants were made in accordance with s 19 • applications for retrieval warrants were made in accordance with s 22 • applications for emergency authorisations and subsequent applications to an eligible Judge or a nominated Administrative Appeals Tribunal member were made in accordance with ss 28, 29, 30 and 33 • written records for emergency authorisations were properly issued in accordance with s 31 • applications for tracking device authorisations and retrieval of tracking devices were made in accordance with s 39 • tracking device authorisations were properly issued in accordance with ss 39 and 40 • warrants were revoked in accordance with ss 20 and 21.

Inspection focus (1): *Were surveillance devices used in accordance with the Act?*		
Relevant Criteria	**Procedural checks**	**Records-based checks**
2. Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?	We check the agency has policies and procedures to ensure: • surveillance devices are used lawfully • it has an auditable system for maintaining surveillance devices • there are sufficient systems in place for capturing the use of surveillance devices • conditions on warrants are adhered to.	We inspect the records and reports relating to the use of surveillance devices against corresponding authorisations and warrants, to assess whether: • use of surveillance devices under a warrant was in accordance with s 18 • use of surveillance devices under an emergency authorisation was in accordance with ss 32 and 18 • retrieval of surveillance devices or tracking devices was carried out in accordance with ss 26 and 39(11) • use of tracking devices under a tracking device authorisation was in accordance with s 39 • any extraterritorial surveillance was in accordance with s 42. In making this assessment, we may also test the veracity of the records by, for example, comparing the details of the records to the information maintained in the systems used by the agency to capture information from surveillance devices. We may also rely on what we understand of an agency's processes and procedures in determining the veracity of such records and take into consideration whether the records were made contemporaneously.

Inspection focus (2): *Is protected information properly managed?*		
Relevant Criteria	**Procedural checks**	**Records-based checks**
3. Was protected information properly stored, used and disclosed?	We check the agency has policies and procedures to ensure: • protected information is kept securely in accordance with the Act • protected information is used and disclosed in accordance with the Act • a person's privacy is protected.	We inspect the records and reports regarding the use and disclosure of protected information that are required under the Act to assess whether anything indicates the agency has used and/or communicated protected information for a purpose other than one outlined in s 45(4).
4. Was protected information properly destroyed and/or retained?	We check the agency has policies and procedures to ensure: • protected information is destroyed in accordance with the Act • protected information is retained in accordance with the Act • protected information is regularly reviewed to assess whether it is still required.	We inspect the records relating to the review, retention and destruction of protected information, including the chief officer's, or delegate's certification that protected information can be retained or destroyed (s 46).

Inspection focus (3): *Was the agency transparent and were reports properly made?*		
Relevant Criteria	**Procedural checks**	**Records-based checks**
5. Were all records kept in accordance with the Act?	We check the agency has policies and procedures to ensure: • it meets its record keeping requirements • it maintains an accurate general register.	We inspect the records presented at the inspection to assess whether the agency has met its record keeping requirements under ss 51 and 52. In assessing whether the agency has met the requirements under s 53 to keep a register of warrants and authorisations, we cross-check the information contained in the register against the corresponding original records.
6. Were reports properly made?	We check the agency has policies and procedures to ensure it accurately reports to the Attorney-General and our Office.	We inspect the copies of reports presented at the inspection to assess whether the agency has met its reporting requirements under ss 49 and 50. In conducting this assessment, we cross-check the information contained in the reports against the corresponding original records.
7. Was the agency cooperative and frank?	Under this criterion we consider: the agency's responsiveness and receptiveness to our inspection findings—whether it has internal reporting mechanisms regarding instances of non-compliance, any self-disclosures the agency may have made to our Office and the Minister and the agency's overall attitude towards compliance.	