Commonwealth OMBUDSMAN

Report to the Attorney-General on agencies' compliance with the *Surveillance Devices Act 2004*

For the period 1 January to 30 June 2015

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 January to 30 June 2014

AUSTRALIAN CRIME COMMISSION
Records from 1 January to 30 June 2014

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2014

CRIME AND CORRUPTION COMMISSION
Records from 1 July 2013 to 30 June 2014

SOUTH AUSTRALIA POLICE
Records from 1 July 2012 to 30 June 2013

WESTERN AUSTRALIA POLICE
Records from 1 July 2013 to 30 June 2014

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

September 2015

Commonwealth OMBUDSMAN

Report to the Attorney-General on agencies' compliance with the *Surveillance Devices Act 2004*

For the period 1 January to 30 June 2015

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 January to 30 June 2014

AUSTRALIAN CRIME COMMISSION
Records from 1 January to 30 June 2014

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2014

CRIME AND CORRUPTION COMMISSION
Records from 1 July 2013 to 30 June 2014

SOUTH AUSTRALIA POLICE
Records from 1 July 2012 to 30 June 2013

WESTERN AUSTRALIA POLICE
Records from 1 July 2013 to 30 June 2014

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

September 2015

ISSN 1833-9263

Contact us
Inquiries 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

INTRODUCTION

The *Surveillance Devices Act 2004* (the Act) regulates the use of surveillance devices by law enforcement agencies.[1] Broadly speaking, the Act allows certain surveillance activities to be conducted 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. It also imposes reporting obligations on law enforcement agencies to ensure an appropriate level of transparency.

What we do

The Commonwealth Ombudsman (Ombudsman) performs the independent oversight mechanism included 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 Commonwealth Attorney-General) at six-monthly intervals. This report sets out the results of our inspections finalised between 1 January and 30 June 2015.

Why we oversee agencies

The use of surveillance devices is one of the most intrusive covert powers afforded to law enforcement agencies, and part of the Ombudsman's role is to provide the Minister and the public with assurance that agencies are using their powers as Parliament intended, and if not, hold the agencies accountable to the Minister and the public.

How we oversee agencies

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

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

[1] Under 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).

We form our assessments based on the records made available at the inspection, discussions with relevant teams, processes we observe and information staff provide in response to any identified issues. To ensure that 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 the agency to identify sources of information to demonstrate compliance. We can rely on coercive powers to obtain any information relevant to the inspection.

We also encourage agencies to be upfront and self-disclose any instances of non-compliance to our office and inform us of any remedial action the agency has taken.

At the end of each inspection we provide our preliminary findings to the agency to enable the agency to take any immediate remedial action.

We may also assist agencies in ensuring compliance through assessing agencies' policies and procedures, communicating 'best-practices' in compliance, and engaging with agencies outside of the 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. Were applications for warrants and authorisations properly made?
2. Were authorisations properly issued?
3. Were surveillance devices used lawfully?
4. Were revocations of warrants properly made?
5. Were records properly kept by the agency?
6. Were reports properly made by the agency?
7. Was protected information properly dealt with by the agency?

Appendix A provides details on our criteria.

How we report

After an inspection, agencies are provided with detailed inspection reports. To ensure procedural fairness we provide a draft report on our findings to the agency for comment before it is finalised. The finalised reports are desensitised and form the basis of our reports to the Minister. Inspection results are considered finalised once the Ombudsman's internal report to the agency is completed, so typically there will be some delay between the date of inspection and the report 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 issues resulting from these inspections.

We may also discuss issues other than instances of non-compliance, such as the adequacies of an agency's policies and procedures to ensure compliance with the Act. Examples of what we may not include in this report are administrative issues or instances of non-compliance where the consequences are negligible, such as where it did not result in unnecessary privacy intrusion.

Relevant agencies

This report includes the results of our inspection of the Australian Commission for Law Enforcement Integrity (ACLEI), Australian Crime Commission (ACC), Australian Federal Police (AFP), Crime and Corruption Commission Queensland (CCC), South Australia Police (SA Police) and Western Australia Police (WA Police). These agencies are defined as a 'law enforcement agency' under s 6(1) of the Act.

Inspection findings overview

The following table provides an overview of all of inspection findings across each agency.

Agency	Australian Commission for Law Enforcement Integrity	Australian Crime Commission	Australian Federal Police
Inspection period[2]	1 January to 30 June 2014	1 January to 30 June 2014	1 January to 30 June 2014
Number of records inspected	7/7 warrants	47/103 (total warrants) 43/49 executed warrants 41/43 retentions	71/332 (total warrants) 71/160 executed warrants 64/153 destructions 24/24 retentions
Criteria	***Inspection findings***		
1. Were applications for warrants and authorisations properly made?	Compliant.	Compliant.	Compliant with one exception.
2. Were authorisations properly issued?	No authorisations were relevant to this inspection period.	Compliant.	Compliant.
3. Were surveillance devices used lawfully?	Nothing to indicate otherwise; however unable to determine in one instance.	Nothing to indicate otherwise; however unable to determine compliance in two instances.	Nothing to indicate otherwise except in one instance. Unable to determine compliance in two instances. One issue discussed.
4. Were revocations of warrants properly made?	No revocations were made during this inspection period.	Compliant.	Compliant with two exceptions.
5. Were records properly kept by the agency?	Compliant.	Compliant.	Compliant.
6. Were reports properly made by the agency?	Compliant with one exception.	Compliant.	Compliant with four exceptions.
7. Was protected information properly dealt with by the agency?	Nothing to indicate otherwise.	Nothing to indicate otherwise. The ACC self-disclosed one instance where protected information was destroyed without the chief officer's approval.	Nothing to indicate otherwise except in 10 instances.

[2] Inspection period refers to the period during which warrants and authorisations either expired or were revoked.

Agency	Crime and Corruption Commission Queensland	South Australia Police	Western Australia Police
Inspection period	1 July 2013 to 30 June 2014	1 July 2012 to 30 June 2013	1 July 2013 to 30 June 2014
Number of records inspected	1/1 warrant	9/9 warrants	2/2 warrants
Criteria	***Inspection findings***		
1. Were applications for warrants and authorisations properly made?	Compliant.	Compliant.	Compliant.[3]
2. Were authorisations properly issued?	No authorisations were relevant to this inspection period.	No authorisations were relevant to this inspection period.	No authorisations were relevant to this inspection period.
3. Were surveillance devices used lawfully?	The warrant was not executed, therefore no assessment was made.	Nothing to indicate otherwise, however key records were unavailable for three warrants.	No surveillance devices were used, therefore no assessment was made.
4. Were revocations of warrants properly made?	No revocations were made during this inspection period.	No revocations were made during this inspection period.	No revocations were made during this inspection period.
5. Were records properly kept by the agency?	Compliant.	Not compliant with some of the requirements under s 53. Not compliant with s 51(a) for warrants issued during 2005-06.	Compliant.
6. Were reports properly made by the agency?	Compliant.	Compliant. Two administrative errors noted.	Compliant with one exception.
7. Was protected information properly dealt with by the agency?	Nothing to indicate otherwise.	Not compliant with ss 52(1)(e) and 46.	Nothing to indicate otherwise.

[3] This criterion refers to applications that resulted in warrants.

FINDINGS

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

We conducted our inspection at ACLEI from 17 to 18 September 2014 in Canberra. Although no recommendations were made as a result of the inspection we were unable to determine compliance in one instance, which is discussed below. We would like to acknowledge ACLEI's cooperation during the inspection.

Issues from previous inspections

It is our usual practice to follow up outstanding or unresolved issues raised in previous inspection findings; however, no issues required follow up at the September 2014 inspection.

Inspection findings

Finding 1

What the Act allows
Section 18(1)(c) of the Act states that a warrant may authorise 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. Section 18(2)(c)(i) of the Act states that this type of warrant authorises the installation, use and maintenance of devices on premises where the person is reasonably believed to be or likely to be.

Section 6 of the Act defines a 'premises' to include: land; a building or vehicle; a part of a building or vehicle; and any place, whether built on or not, within or beyond Australia.

What we found
For one warrant, records indicated that a surveillance device was installed on a portable object identified as being used by the person listed on the warrant, rather than being installed at a premises. A portable object would not meet the definition of 'premises' under s 6 of the Act.

If ACLEI were able to demonstrate, for example, that the portable object was always in the possession of the person and therefore co-located at a premises with the person, then we would have been able to provide a higher level of assurance that the device was used in accordance with s 18(2)(c)(i). However, based on the records available at the inspection we

were unable to determine this.

Further information provided by ACLEI
Subsequent to the inspection ACLEI advised that it had in place a concurrent warrant obtained under different legislation from which it could be confirmed that the person listed on the warrant was in possession of the portable object when the device was used.

Suggested practice
To ensure that the use of a surveillance device on a portable object is authorised at all times, ACLEI may consider applying for a warrant in respect of both the person and the portable object. Alternatively, if it is not known what portable objects are being used by the person prior to the warrant being granted, ACLEI may consider making an application to vary the warrant to include the portable object.

AUSTRALIAN CRIME COMMISSION

We conducted our inspection at the ACC from 7 to 9 October 2014 in Brisbane. Although no recommendations were made as a result of the inspection, we were unable to determine compliance in two instances and the ACC self-disclosed an instance of non-compliance, which are further discussed below. However, we are satisfied that the ACC has taken self-initiated measures to address these issues.

We would also like to acknowledge the ACC's cooperation during the inspection and for its ongoing frank and open engagement with our office.

Issues from previous inspections

It is our usual practice to follow up outstanding or unresolved issues raised in previous inspection findings; however, no issues required follow up at the October 2014 inspection.

Inspection findings

In addition to our inspection findings discussed below, we noted detailed records demonstrating how the ACC ensured that surveillance devices were used in accordance with warrants issued in respect of persons whose identity had not yet been confirmed. In these instances, we can provide a higher level of assurance that the ACC had used surveillance devices in accordance with the warrants.

Finding 1

What the Act allows
Section 18(1)(c) of the Act states that a warrant may authorise 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. Section 18(2)(c)(i) of the Act states that this type of warrant authorises the installation, use and maintenance of devices on premises where the person is reasonably believed to be or likely to be.

What we found and the ACC's response
For one warrant, we were unable to confirm that a surveillance device was used at a premises where the person named on the warrant was reasonably believed to be. We were therefore unable to determine compliance. Subsequent to the inspection, we received verbal advice from the investigator regarding why there was a reasonable belief that the person would be located at the premises where the device was used.

For another warrant, there were conflicting records on file regarding what type of device was used. We requested clarification from the ACC regarding which device was used, as this would determine the type of information we would require to determine compliance with s 18(2)(c)(i) of the Act. The ACC acknowledged that there was a reporting error, provided clarification and made available records indicating that the surveillance device was used lawfully. As the ACC had also incorrectly reported to the Minister on its surveillance activities under this warrant, under s 49 of the Act, it sent an amended report.

Finding 2

What the Act requires
Under s 46(1)(b) of the Act, as soon as practicable after a record or report comprising protected information is made, the chief officer must ensure that the record or report is destroyed if the chief officer is satisfied that it is no longer required by the law enforcement agency.

Self-disclosed issue
The ACC informed our office that protected information obtained under two warrants issued to the ACC had been destroyed without the chief officer first being satisfied that the protected information was no longer required. The ACC advised that the protected information was destroyed by members of a state police force, who executed the warrants as a part of a joint agency operation.

The ACC indicated that this most likely occurred due to this agency having a different storage procedure and destruction policy to the ACC. However, as the warrants authorising the use of the devices were issued to the ACC, it was ultimately the ACC's responsibility to deal with the protected information in accordance with the Act.

ACC's advised remedial action
In recognising its responsibilities, the ACC advised that, to prevent reoccurrences of this in the future, it will remind investigators of other agencies of the destruction and reporting requirements of the Act, and potentially reflect this in joint agency agreements prior to the commencement of an investigation. It also advised that it is reviewing its current templates and undertaking negotiations with relevant partner agencies.

We acknowledge the ACC's disclosure of this matter and ongoing transparency with our office, as well as its demonstrated understanding of its requirements under the Act.

AUSTRALIAN FEDERAL POLICE

We conducted our inspection at the AFP from 13 to 16 October 2014 in Canberra. Although no recommendations were made as a result of the inspection, we identified a small number of instances of non-compliance and were unable to determine compliance in two instances, which are further discussed below. However, we note the AFP's self-initiated measures to address some of these issues.

We would also like to acknowledge the AFP for its cooperation during the inspection, particularly from its technical specialists who provided our office with information regarding some of the internal processes and accountability measures the AFP has in place when using surveillance devices under the Act.

Issues from previous inspections

In our last report to the Minister we discussed three issues identified at the March 2014 inspection. The same three findings were identified at the October 2014 inspection and are discussed under *Inspection findings*.

The measures taken by the AFP to address these instances are also discussed.

The finding discussed under Finding 2 (over the page) related to insufficient records to determine that the installation, use and maintenance of devices was in accordance with certain warrants.

As we have reported on this issue a number of times, subsequent to the October 2014 inspection we sought information from AFP technical specialists regarding their processes when using surveillance devices under these warrants. This information has enabled us to more conclusively determine whether the actions taken by the AFP were authorised and has informed our assessments at subsequent inspections. We acknowledge the AFP's frankness and cooperation in this regard.

Inspection findings

In addition to the findings discussed below, the AFP incorrectly reported to our office and the Minister that a warrant had not been executed, when it had been. There were no records on file to indicate that surveillance devices had been used under the authority of the warrant, but, through the course of

conducting our assessments, it became apparent that there had been surveillance activities.

In addition to inaccurate reporting on surveillance activities to the Minister, such errors also impact on our sampling methodologies for inspections, where we consider whether or not a warrant has been executed. In accepting this finding, the AFP was able to explain why this error occurred, and based on its advised remedial action, we have more confidence in its procedures going forward.

Finding 1

What the Act allows
Section 17(1A)(1) of the Act states that a warrant may only be issued for a period of no more than 90 days. Section 18 of the Act outlines what a warrant authorises during the 90 day period, including the installation, use and retrieval of surveillance devices.

What we found
We identified one instance where a surveillance device was used after the warrant authorising the use of that device had expired.

Remedial action taken by the AFP
Once the AFP identified this issue, it disabled the device as soon as possible. The AFP also reviewed and updated its administrative processes to ensure that this situation does not occur again.

Finding 2

What the Act allows
Section 18(1)(c) of the Act states that a warrant may authorise 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. Section 18(2)(c)(i) of the Act states that this type of warrant authorises the installation, use and maintenance of devices on premises where the person is reasonably believed to be or likely to be.

What we found
For two warrants, we were unable to confirm that a surveillance device was used at a premises where the person named on the warrant was reasonably believed to be. We were therefore unable to determine compliance with s 18(2)(c)(i) of the Act.

In one of these instances, the power conferred by the warrant was exercised by another agency on behalf of the AFP and therefore we could not rely on the relevant AFP procedures.

Further information provided by the AFP
Subsequent to the inspection, the AFP advised that it was satisfied that the devices were used in accordance with s 18(2)(c)(i) of the Act, and for one of the warrants, it sent an amended report to the Minister under s 49 of the Act relating to the relevant surveillance activities.

Finding 3

What the Act requires
Under s 46(1)(b) of the Act, as soon as practicable after a record or report comprising protected information is made, the chief officer must ensure that the record or report is destroyed if the chief officer is satisfied that it is no longer required by the law enforcement agency. The chief officer may certify to retain protected information if satisfied that it is still likely to be required. The decision to retain or destroy protected information must be made within five years after its creation. If the chief officer decides to retain protected information, the decision must be made every five years until the protected information is destroyed. An exception to this is under s 46(3) of the Act, where protected information is received into evidence in a legal or disciplinary proceeding.

What we found
We identified that protected information obtained under 10 warrants had been kept for a period longer than five years without the chief officer certifying that it could be retained.

The AFP's advised remedial action
In response to this finding the AFP advised that it is developing formal guidance on the destruction of protected information, to assist relevant staff to understand their legislative responsibilities.

Crime and Corruption Commission

We conducted our inspection at the CCC on 28 August 2014 in Brisbane. No recommendations were made as a result of the inspection and no issues were identified. We would also like to acknowledge the CCC's cooperation during the inspection.

Issues from previous inspections

During our previous inspection at the CCC, we noted that it was in the process of developing a policy regarding the issuance of warrants and management of protected information, to ensure compliance with the Act.

Following this inspection, the CCC confirmed that it had either developed, or had in draft form, such policies and procedures. The CCC also advised that it was in the process of creating additional guidance documents relating to the warrant application process.

We will report on any further progress made by the CCC in finalising and developing these procedures in our next report.

SOUTH AUSTRALIA POLICE

We conducted our inspection at the South Australia Police from 11 to 13 August 2014 in Adelaide. Although no recommendations were made as a result of this inspection, we identified a small number of non-compliances, which are discussed below. We note that the South Australia Police has advised of appropriate remedial action.

We would like to acknowledge the South Australia Police's cooperation during the inspection and responsiveness to our inspection findings.

Issues from previous inspections

Three recommendations were made as a result of our previous inspection, which was conducted in 2006 and reported on to the Minister in 2007:

Recommendation 1: *The SA Police should ensure that the report sent to the Minister under s 49(1) of the Act includes all the information required by s 49(2).*

Recommendation 2: *The SA Police should ensure that once the need for a surveillance device ceases all revocations are promptly signed by an appropriate officer.*

Recommendation 3: *The SA Police should ensure that an instrument of delegation is signed by the Commissioner as chief officer under s 63 of the Act to authorise persons of appropriate rank to exercise the Commissioner's powers and functions under the Act.*

None of the issues relating to these recommendations were identified at the August 2014 inspection.

Other issues

In our last report we noted that the South Australia Police's records regarding its use of the Act were held across three separate locations and that dispersed material may have become difficult to administer if the South Australia Police's use of the Act increased. Prior to the August 2014 inspection, the South Australia Police advised that it now centrally administers its records relating to the use of surveillance devices under the Act.

We also made a best practice suggestion for the South Australia Police to introduce contemporaneously made records when installing, using and retrieving surveillance devices to better demonstrate what actions were taken under a warrant and to assist the South Australia Police with its reporting requirements. At the August 2014 inspection we noted that such records were provided for six out of nine warrants. For the remaining three warrants, we had to rely on reports on surveillance activities made at a later date.

We consider contemporaneous records to be the best source of evidence to determine whether surveillance devices were used lawfully. The South Australia Police accepted this finding and advised that it will ensure that such records are provided for future warrants.

Inspection findings

The first two findings relate to record keeping requirements imposed by the Act, which ensure that agencies are transparent in their use of surveillance devices. The record keeping requirements also our assist our office in determining agencies' compliance with the Act more broadly. The third finding relates to the proper handling of information obtained from the use of surveillance devices.

Finding 1

What the Act requires
Section 51 of the Act requires the chief officer of a law enforcement agency to keep each warrant and tracking device authorisation. Section 53(1) of the Act requires the chief officer of a law enforcement agency to keep a register of all warrants and authorisations sought by the agency, and s 53(2) of the Act specifies the details that need to be kept on the register about each warrant and authorisation.

What we found
For all warrants, not all information required under s 53(2) of the Act was recorded on the register.

For the warrants and tracking device authorisation relevant to our previous inspection, none of the information required under s 53(2) of the Act was recorded on the register. Additionally, the South Australia Police could not locate the warrants and authorisation and therefore could not demonstrate compliance with s 51 of the Act.

The South Australia Police advised that prior to 2012 it did not have a specific policy in relation to the administration of warrants obtained under the Act.

South Australia Police's advised remedial action
The South Australia Police accepted these findings and advised that it introduced a new policy that provides clear direction for the management and retention of warrants to ensure strict compliance. It also updated the register to include all required information for the warrants relevant to the August 2014 inspection.

Finding 2

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 or authorisation, as per s 44(1)(a) of the Act.

Section 52(1)(e) of the Act requires an agency to keep details of each use of information obtained from the use of a surveillance device by a law enforcement officer of the agency.

What we found
For all warrants, records indicated that surveillance devices had been used, but there were no records available regarding the use of the protected information obtained from these devices.

In order to assess compliance with s 52(1)(e) of the Act, we need to understand how an agency manages and stores protected information and be able to test that these processes are working. It appeared that the South Australia Police was unable to provide this at the inspection.

South Australia Police's advised remedial action
The South Australia Police accepted this finding and advised that it has implemented a procedure for this information to be captured both on physical and electronic records.

Finding 3

What the Act requires
Under s 46(1)(b) of the Act, as soon as practicable after a record or report comprising protected information is made, the chief officer must ensure that the record or report is destroyed if the chief officer is satisfied that it is no longer required by the law enforcement agency. The chief officer may certify to retain protected information if satisfied that it is still likely to be

required. The decision to retain or destroy protected information must be made within five years after its creation. If the chief officer decides to retain protected information, the decision must be made every five years until the protected information is destroyed. An exception to this is under s 46(3) of the Act, where protected information is received into evidence in a legal or disciplinary proceeding.

What we found

As noted under Finding 1, the South Australia Police could not locate the warrants or authorisation issued before 1 July 2006. If protected information had been obtained as a result of using surveillance devices under these warrants and authorisation, the chief officer would have been required to have either retained or destroyed the protected information by 30 June 2011 at the latest.

There were no records to demonstrate that the chief officer had given consideration to the destruction or retention of this protected information, and whether any protected information had been destroyed.

South Australia Police's advised remedial action

As noted above, the South Australia Police has recently centralised its record keeping procedures, which should reduce the likelihood of warrant and authorisation records becoming misplaced in the future.

WESTERN AUSTRALIA POLICE

This was our first inspection of the Western Australia Police under the Act, which was held on 29 July 2014 in Perth. No recommendations were made as a result of the inspection and no significant issues were identified; however, we did make one best-practice suggestion, as discussed below.

At the time of the inspection, the Western Australia Police did not have formal guidance in place for its officers when applying the provisions of the Act. Noting that it already had guidance in place for corresponding state legislation and sound administrative processes, we suggested that the Western Australia Police formalise its guidance to ensure compliance with this Act. Subsequent to the inspection, the Western Australia Police advised that it introduced formal guidance. We commend the Western Australia Police for its responsiveness.

We would also like to acknowledge the Western Australia Police's cooperation during the inspection and for being forthcoming in providing detailed contemporaneous records that assisted our office in forming our compliance assessment.

APPENDIX A – INSPECTION CRITERIA

1. **Were applications for warrants and authorisations properly made?**

   Under this criterion, we assess agency compliance with the following provisions of the Act:

   - making applications for surveillance device warrants under s 14
   - making applications for extensions/variations to surveillance device warrants under s 19
   - making applications for retrieval warrants under s 22
   - making applications for emergency authorisations and subsequent applications to an eligible Judge or a nominated AAT member under ss 28, 29 and 33
   - making applications for tracking device authorisations and retrieval of tracking devices under s 39
   - keeping each document required by s 51(e) to (h).

2. **Were authorisations properly issued?**

   Under this criterion, we assess agency compliance with the following provisions of the Act:

   - written records for emergency authorisations were properly issued under s 31 and each written record of the authorisation was kept in accordance with s 51(c)
   - tracking device authorisations were properly issued under ss 39 and 40, and each written record of the authorisation was kept in accordance with s 51(d)
   - authorisations for the retrieval of tracking devices were properly issued under ss 39 and 40.

3. Were surveillance devices used lawfully?

Under this criterion, we assess agency compliance with the following provisions of the Act:

- whether surveillance devices were used in accordance with the relevant warrant (s 18)
- whether surveillance devices were used in accordance with the relevant emergency authorisation (ss 18 and 32)
- whether retrieval of surveillance devices or tracking devices was carried out lawfully (ss 26 and 39(11))
- whether tracking devices were used in accordance with the relevant tracking device authorisation (s 39)
- whether extra-territorial surveillance was carried out lawfully (s 42).

4. Were revocations of warrants properly made?

Under this criterion, we assess agency compliance with the following provisions of the Act:

- revoking warrants under ss 20, 21 and 27 and
- keeping records of revocation under s 51(b).

5. Were records properly kept by the agency?

Under this criterion, we assess agency compliance with the following provisions of the Act:

- keeping the register under s 53
- keeping each warrant under s 51(a)
- keeping evidentiary certificates under s 51(k)
- keeping documents under s 52(1)(a) – (d).

6. Were reports properly made by the agency?

Under this criterion, we assess agency compliance with the following provisions of the Act:

- reporting to the Attorney-General under s 49 after the warrant ceased to be in force and keeping each report under s 51(j)
- reporting annually to the Attorney-General under s 50.

7. Was protected information properly dealt with by the agency?

Under this criterion, we assess the AFP's compliance with the following provisions of the Act:

- dealing with protected information under ss 46(1)(a) and 52(1)(e) to (h)
- destroying and retaining protected information under ss 46(1)(b) and 52(1)(j).