



AFP Practical Guide (ACT Policing) on surveillance devices

Metadata	
Caption	Surveillance Devices (ACT Policing)
Document Identifier	PRA10120
Description	AFP Practical Guide (ACT Policing) on surveillance devices
Governance Function	Community Policing
Owned by	Chief Police Officer ACT Policing
Date First Approved	8/03/2011 12:00 AM
Contact Person	Superintendent Criminal Investigations
Date Published	11/05/2011 12:00 AM
Date Modified	26/9/2011
Date Last Reviewed	8/03/2011 12:00 AM
Authorised by	Chief Police Officer ACT Policing
Date of Next Review	8/03/2013 12:00 AM
Review Notification	'ACT-Policing-Governance@afp.gov.au'
Instrument Type	Practical Guide
Replaces	
Stakeholders	ACT Policing
Instrument Classification	UNCLASSIFIED

1. Disclosure and compliance

This document is classified **UNCLASSIFIED** and is intended for internal AFP use.

Disclosing any content must comply with Commonwealth law and the [AFP National Guideline on disclosure of information](#).

Compliance

This instrument is part of the AFP's professional standards framework. The [AFP Commissioner's Order on Professional Standards \(CO2\)](#) outlines the expectations for appointees to adhere to the requirements of the framework. Inappropriate departures from the provisions of this instrument may constitute a breach of AFP professional standards and be dealt with under Part V of the [Australian Federal Police Act 1979](#) (Cth).

2. Acronyms

AFP	Australian Federal Police
CPO	Chief Police Officer
DPP	Director of Public Prosecutions (ACT)

s37(2)(a), 37(1)(c), s47E(d)

3. Definitions

Application - the process for seeking a surveillance device warrant (including a tracking device warrant), an approval of emergency authorisation, a retrieval warrant and a revocation.

Appointees - defined in s. 4 of the *Australian Federal Police Act 1979* (Cth) and are, if sworn, 'law enforcement officers' under the *Crimes (Surveillance Devices) Act 2010* and the *Surveillance Devices Act 2004* (Cth).

Authorisation - the process whereby a person who is appropriately authorised approves an application for a warrant, revocation or an emergency authorisation.

Corresponding emergency authorisation - an authorisation given under the provisions of a corresponding law that correspond to Part 3 (Emergency Authorisations) of the *Crimes (Surveillance Devices) Act 2010*.

Corresponding law - a law of another jurisdiction that corresponds to the *Crimes (Surveillance Devices) Act 2010*, and includes a law of another jurisdiction that is declared by regulation to correspond to the *Crimes (Surveillance Devices) Act 2010*.

Corresponding warrant - a warrant issued under provisions of a corresponding law that corresponds to Part 2 (Warrants) of the *Crimes (Surveillance Devices) Act 2010*.

Data surveillance device - a device or program capable of being used to record or monitor the input of information into or the output of information from a computer but does not include an optical surveillance device.

Device - includes an instrument, apparatus and equipment.

Emergency authorisation - an emergency authorisation given under Part 3 (Emergency Authorisation) of the *Crimes (Surveillance Devices) Act 2010*.

Enhancement equipment - (in relation to a surveillance device) equipment that can enhance

a signal, image or other information obtained by using the device.

Listening device - any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but not including a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and to permit that person to hear only sounds ordinarily audible to the human ear.

Maintain - (in relation to a surveillance device) adjust, relocate, repair or service a device and replace a faulty device.

Optical surveillance device - any device capable of being used to record visually or observe an activity, but not including spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.

Participating jurisdiction - a jurisdiction in which a corresponding law is in force.

Premises - include, whether in or beyond the ACT:

- land
- a building or vehicle
- a part of a building or vehicle
- any place, whether built on or not.

Protected information - information, under the *Crimes (Surveillance Devices) Act 2010*, that is:

- obtained by using a surveillance device under warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation
- relating to an application for, issuing, existence or expiry of a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation
- an application to approve an exercise of power under an emergency authorisation
- an application under a corresponding law to approve an exercise of power under a corresponding emergency authorisation.

Record - includes a:

- visual, audio, or audiovisual record
- record in digital form
- documentary record prepared from a record of the type herein described.

Relevant offence - an offence against an ACT law punishable by imprisonment of three years or more, or an offence against an ACT law prescribed by regulation.

Relevant proceeding - includes:

- prosecuting a relevant offence
- a proceeding to protect a child or intellectually impaired person
- a proceeding to confiscate, forfeit or restrain property
- a coronial inquest or inquiry into a matter resulting from the commission of a relevant offence
- extradition proceedings for a person into the ACT, to the extent that the proceeding relates to a relevant offence.

Retrieval warrant - a warrant issued under Division 2.3 of Part 2 of the *Crimes (Surveillance Devices) Act 2010* to authorise the retrieval of a surveillance device.

Surveillance device - a data surveillance device, a listening device, an optical surveillance device, a tracking device, or a device of a kind prescribed by the regulations. The definition also includes a device that is a combination of any two or more of the four specified types of device.

Surveillance device warrant - a warrant issued under Division 2.2 (Surveillance device warrants) or s. 29(3) (Judge may approve emergency use of powers) of the *Crimes (Surveillance Devices) Act 2010*.

Tracking device - any electronic device capable of being used to work out or monitor the location of a person or an object or the status of an object.

4. Authority to create guideline

This guideline was issued by the Chief Police Officer for the ACT using power under s. 37(1) of the *Australian Federal Police Act 1979* (Cth) as delegated by the Commissioner under s. 69C of that Act.

5. Introduction

This guideline outlines policies and procedures for ACT Policing appointees to lawfully deploy surveillance devices (not telecommunications interception devices) to investigate ACT-specific offences under the ACT [Crimes \(Surveillance Devices\) Act 2010](#) ('the Act').

Appointees must also comply with the [AFP National Guideline on Surveillance Devices](#) and, when investigating Commonwealth matters, the *Surveillance Devices Act 2004* (Cth).

6. Legislation

Appointees should refer to additional advice in the ACT Policing

s37(2)(b)

Telecommunications Interception warrants must be applied for, and issued, under the [Telecommunications \(Interception and Access\) Act 1979](#) (Cth).

Appointees must note that the Act does not include any transitional provisions for warrants issued under the *Australian Federal Police Act 1979* (Cth) by virtue of the transitional provisions of the *Surveillance Devices Act 2004* (Cth). Warrants issued under those Acts fall under a Commonwealth regime, whereas the ACT *Crimes (Surveillance Devices) Act 2010* is an entirely ACT-based regime.

The Commonwealth legislation under which warrants were previously issued remains valid but new warrants must only be sought in the ACT through the ACT *Crimes (Surveillance Devices) Act 2010*. Warrants issued to ACT Policing appointees under the *Australian Federal Police Act 1979* (Cth) and in force before the *Crimes (Surveillance Devices) Act 2010* commences remain valid while they are active. If extensions or amendments to these Commonwealth warrants are sought in the ACT, applications for new warrants will need to be made in accordance with the

provisions of the ACT *Crimes (Surveillance Devices) Act 2010*.

The Act recognises corresponding laws of other jurisdictions so that a surveillance device warrant or emergency authorisation authorised in another jurisdiction may, by virtue of a corresponding law, be executed in the ACT as if it were issued under Part 2 (Warrants) of the Act or an emergency authorisation given under Part 3 (Emergency authorisations) of the Act.

Appointees should make themselves familiar with the dictionary of the Act.

7. ACT DPP role

ACT Policing must continue to use procedures established for all Special Projects applications. The Office of the ACT Director of Public Prosecutions (DPP) vets and notarises draft documents and appears with applicants before judges or magistrates when ACT Policing appointees apply for surveillance device warrants.

The DPP will, under the [Memorandum of Understanding between AFP and Commonwealth DPP](#) and s. 40(h) of the Act, try to advise ACT Policing of each occasion when information obtained with a surveillance device was given in evidence in a relevant proceeding.

8. Procedures

Appointees should follow the procedures set out s37(2)(b)

9. Surveillance devices without a warrant or authorisation

Appointees who want to use a surveillance device to collect evidence for an investigation covered by the Act must:

- apply for a warrant unless the Act states it is not required
- note that material obtained without a warrant when one was available, or should have been obtained, is generally inadmissible.

Appointees need not obtain a warrant to use an optical surveillance device if the device can be used in a place where the presence of a police officer is not an offence (e.g. using binoculars/cameras in a public place or on private property with the consent of the occupier, per s. 7(3) of the Act).

Appointees must note that Part 4 of the *Surveillance Devices Act 2004* (Cth) permits using a surveillance device, without warrant, for listening to or recording a person's speech, if the appointee (or a person assisting them) speaks the words or is a person who the speaker intends or should reasonably expect the words to be heard by (per Section 38).

9.1 Use of tracking devices

Tracking devices must only be used when authorised by a surveillance device warrant.

The ACT legislation does not cover appointees using a tracking device without warrant, unlike the *Surveillance Devices Act 2004* (Cth).

Appointees must only use a tracking device without warrant when authorised by the *Surveillance Devices Act 2004* (Cth) and the [AFP National Guideline on Surveillance Devices](#); this only pertains to relevant offences under that Act and not under the *Crimes (Surveillance Devices) Act 2010*.

10. Using surveillance devices with a warrant

10.1 Offences

Surveillance device warrants under the *Crimes (Surveillance Devices) Act 2010* may be sought for:

- an offence against ACT law punishable by three or more years of imprisonment
- an offence against ACT law prescribed by regulations.

10.2 Activities that can be authorised

Appointees must only seek surveillance device warrants under this Act to use a device:

- on a stated premises, building, land, vehicle or place
- in or on a stated object or class of objects
- in relation to the conversations, activities or geographical location of a stated person or a person whose identity is unknown.

The Act specifies four types of surveillance devices, and appointees must consider the type of surveillance device warrant most appropriate to their investigation. The following types of surveillance device warrants are available:

- warrant for a data surveillance device
 - specified premises, vehicle, or class of vehicle
 - specified object or class of objects
 - specified person
- warrant for a listening device
 - specified premises, vehicle, or class of vehicle
 - specified object or class of objects
 - specified person
- warrant for an optical surveillance device
 - specified premises, vehicle, or class of vehicle
 - specified object or class of objects
 - specified person
- warrant for a tracking device
 - specified premises, vehicle, or class of vehicle
 - specified object or class of objects
 - specified person
- a single warrant covering more than one of the above categories if appropriate in the circumstances of the case.

Appointees wanting to use one surveillance device to record vision and sound must ensure it is clear on the face of the warrant that it authorises both the recording of vision and sound.

10.3 Geographic scope of warrants

A surveillance device warrant under this Act authorises using surveillance devices:

- anywhere in the ACT
- only in another jurisdiction if it is a participating jurisdiction (one in which a law corresponding with this Act operates, including any laws declared by Regulation to correspond to this Act).

For this Act an investigation into a relevant offence is deemed to be conducted in the ACT, whether or not it is also conducted in another jurisdiction, if an appointee participates in the investigation. For example, it covers an ACT Policing member conducting or participating in an investigation wholly conducted in another jurisdiction but for an ACT offence (e.g. conspiracy to import drugs from NSW into the ACT where all the evidence is in NSW).

Section 31 of the Act permits a corresponding warrant from another jurisdiction to be executed in the ACT as if it were a surveillance device warrant or retrieval warrant issued under Part 2 of the Act.

10.4 Powers under warrants

Specified premises warrants permit appointees to enter, by force if necessary, to install, use and maintain a surveillance device in:

- the stated premises
- other stated premises adjoining or providing access to the principal premises.

Specified object warrants permit appointees to enter, by force if necessary, to install, use and maintain a surveillance device in:

- any premises where the object is reasonably believed to be
- other premises adjoining or providing access to the premises where the object is reasonably believed to be.

Specified person warrants permit appointees to enter, by force if necessary, to install, use and maintain a surveillance device in:

- the premises where the person is reasonably believed to be or likely to be
- other premises adjoining or providing access to the premises where the person is reasonably believed to be or likely to be.

Surveillance device warrants also permit appointees to:

- retrieve the surveillance device(s)
- install, use, maintain and retrieve any enhancement equipment
- temporarily remove an object or vehicle from premises to install, maintain or retrieve a surveillance device
- break open anything to install, maintain or retrieve a surveillance device or enhancement equipment
- draw electricity or connect to a system to make a device work
- conceal the fact that anything has been done to install, use, maintain or retrieve a device.

10.5 Retrieval warrant

If a surveillance device must be removed once the surveillance device warrant has expired, appointees must apply for a retrieval warrant (per s. 21 of the Act) using the appropriate application forms.

After a warrant expires or is revoked, surveillance devices must be retrieved unless retrieval risks outweigh the risk of the device being discovered and its technology and/or AFP methodology being compromised.

10.6 Emergency authorisations

Appointees may, in accordance with Part 3 of the Act, apply to the CPO or a person holding the position of Deputy Chief Police Officer for emergency authorisation to:

- use a surveillance device if they reasonably suspect, in the course of investigating a relevant offence, an imminent threat of serious violence to a person or substantial damage to property exists
- continue using a surveillance device (where a surveillance device warrant exists) if the investigation for which a surveillance device is authorised in the ACT is likely to extend to a participating jurisdiction.

Applications can be oral, written, via telephone, fax, email or any other means of communication. Appointees must consult ss. 25-26 of the Act to address application requirements and to understand the powers conferred by such an authorisation.

Appointees seeking emergency authorisations must inform the [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) to ensure accountability requirements are met and the appropriate forms are used.

The authorising officer must make a written record of the authorisation using the appropriate authorisation and record form.

Within two working days after giving an emergency authorisation the CPO, or another AFP appointee on the CPO's behalf (such as the case officer), must apply to an ACT Supreme Court judge to approve that exercise of power under the emergency authorisation. This application must use the appropriate form specific to the type of emergency authorisation ([form 4C](#) for a Section 25 authorisation or [form 4D](#) for a Section 26 authorisation).

The [s37\(2\)\(b\), s37\(1\)\(a\), s47E\(d\)](#) must ensure the preceding requirements are met.

The judge may not approve the authorisation and may then order use of the surveillance device to cease, and instruct how to deal with any:

- information obtained from or relating to the exercise of powers under the emergency authorisation
- record of that information.

This order should be provided to the [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) so that any material collected by the device can be treated as ordered.

The case officer should ensure the device is deactivated and apply for a warrant to retrieve it, noting that such a warrant may not necessarily be granted.

Where appointees seek to retrieve a surveillance device that was installed under an emergency authorisation that is subsequently not approved by a judge, or where a retrieval warrant is sought but not approved, appointees are to consult with the [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) in the first instance.

11. Application process in detail

The internal ACT Policing application process for warrants and emergency authorisations under the Act is managed by the ACT Policing Special Projects Committee using processes established for Special Projects applications.

All administrative documents for surveillance devices must be vetted [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) to ensure compliance with guidelines and reporting requirements.

11.1 Investigation Case Officer responsibilities

Each operation shall have a nominated case officer.

A case officer must, in consultation with [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) :

- discuss the appropriateness and feasibility of seeking a warrant
- consider the:
 - relevant background information
 - rationale for the surveillance device(s) sought
 - lack of alternative means to obtain the information
 - availability of resources to monitor listening devices and to generally act on the information likely to be collected
 - likelihood of foreign language being obtained (necessitating interpreter services)
- produce the draft application, affidavit, warrant and other relevant documents in line with the 'Procedures to obtain a surveillance device warrant (ACT Policing)' guide
- liaise with [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) case officer as often as necessary to ensure both officers are briefed on actual and anticipated developments in the operation and brief the [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) on the requirements of the investigation and of the warrant
- provide written advice and directions, [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) for appraising, installing and retrieving deployed devices
- liaise with [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) at least two weeks before the warrant expires to formulate a device retrieval plan
- notify and liaise immediately with [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) in respect to warrants to be revoked
- provide a copy of the warrant to [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#)
- liaise with [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) for access to product
- ensure their team is briefed on:
 - handling, use and communication procedures for surveillance product to comply with ss. 33-37 of the Act
 - reporting and record-keeping procedures for surveillance product to comply with ss. 38-41 of the Act.

11.2 [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) Case Officer responsibilities

Only s37(2)(b), 37(1)(c), s47E(d) are authorised by this guideline to execute warrants and emergency authorisations.

s37(2)(b), 37(1)(c), s47E(d) must ensure a case officer is identified and allocated to each operation.

s37(2)(b), 37(1)(c), s47E(d) must:

- liaise with the case officer
- appraise, install, maintain and retrieve deployed devices
- submit to the appropriate Functional manager and the s37(2)(b), 37(1)(c), s47E(d) written advice of the failure, retrieval or loss of each deployed device
- record a description of:
 - all devices
 - their deployment
 - date and time of deployment
 - identifying number
 - operation name
 - location of device
 - date of warrant issue
 - duration of issue
 - warrant number
 - name of AFP case officer
 - expiration or revocation of warrant
 - installation, maintenance, retrieval and repair of all deployed devices
- maintain timely liaison with surveillance and operational/investigative personnel
- receive timely briefings from case officers on operational developments affecting installation, use and retrieval of devices
- forward s37(2)(b), 37(1)(c), s47E(d) for recording.

11.3 s37(2)(b), 37(1)(c), s47E(d)

s37(2)(b), 37(1)(c), s47E(d)

12. ACT Policing member application to seek a warrant

Appointees may apply for approval to seek a warrant pursuant to the *Crimes (Surveillance Devices) Act 2010*.

12.1 Special Projects Committee warrant decisions

Applicants seeking Special Projects Committee approval to apply for a warrant must forward to the s37(2)(b), 37(1)(c), s47E(d) :

- a covering minute discussing the appropriateness and feasibility of seeking the warrant, as

outlined in s. 11.1 of this guideline

- the draft application, affidavit, warrant and other documents in line with the 'ACT Policing Procedures to obtain a surveillance device warrant' guide.

If the application is deferred or not approved by the Special Projects Committee, ^{s37(2)(b), 37(1)(c), s47E(d)} must advise the applicant accordingly.

A Special Projects Committee approval process involves:

- the case officer drafting all documents in consultation with ^{s37(2)(b), 37(1)(c), s47E(d)} as outlined above
- ^{s37(2)(b), 37(1)(c), s47E(d)} vetting the affidavit and all application documentation and advising case officer of the changes required
- convening a Special Projects Committee comprising:
 -
 - ^{s37(2)(b), 37(1)(c), s47E(d)}
 -

When the Special Project Committee approves the case officer applying for a warrant, ^{s37(2)(b), 37(1)(c), s47E(d)} must:

- notify the case officer of approval
- instruct the case officer of any amendments to the affidavit or other documents that may be required
- authorise the case officer to liaise with the DPP.

When the Special Project Committee approves the case officer applying for a warrant the case officer must:

- make any necessary amendments to the affidavit or other documents
- ensure all relevant documentation is prepared
- make an appointment to see a DPP Special Projects prosecutor in order to vet and notarise the documents (the case officer is to swear / affirm these documents before the DPP Special Projects prosecutor)
- with the DPP Special Projects prosecutor, make an appointment to see a judge or magistrate to hear the application
- in company with the DPP Special Projects prosecutor, apply for the warrant(s) before the judge or magistrate.

12.2 Action following the decision of a judge or magistrate

The applicant must, after applying to a judge or magistrate for a warrant, notify ^{s37(2)(b), 37(1)(c), s47E(d)} in order to record the application details and outcome (warrant/s issued, refused or withdrawn). This information is to be recorded by the ^{s37(2)(b), 37(1)(c), s47E(d)}

After the applicant appears before a judge or magistrate to seek the issue of the warrant the applicant must:

- scan all original documentation ^{s37(2)(b), 37(1)(c), s47E(d)}
- return all original documentation to ^{s37(2)(b), 37(1)(c), s47E(d)}

- advise s37(2)(b), 37(1)(c), s47E(d) of the judge's or magistrate's decision
- liaise with s37(2)(b), 37(1)(c), s47E(d) to ensure all the provisions of the Act are complied with.

The s37(2)(b), 37(1)(c), s47E(d) must keep records of warrants granted.

13. Responsibilities during the life of the surveillance device warrant

13.1 Execution of warrants and authorisations

s37(2)(b), 37(1)(c), s47E(d) surveillance officers are authorised by this guideline to execute surveillance device warrants solely for tracking devices, and surveillance officers must develop and maintain their skills to use, install and retrieve tracking devices where they do not enter premises or interfere with the interior of a vehicle.

Only s37(2)(b), 37(1)(c), s47E(d) are authorised by this guideline to:

- execute all other surveillance device warrants and emergency authorisations
- develop and maintain their skills in covert methods of entry onto premises and into vehicles, vessels, aircraft and objects.

s37(2)(b), 37(1)(c), s47E(d) can give evidence on maintaining, installing and retrieving surveillance devices (to protect methodology and technology).

Surveillance officers may give evidence on surveillance devices only where tracking devices do not involve entering a vehicle or interfering with the interior of a vehicle.

13.2 Handling of surveillance device product

Appointees must, under the Act, regard surveillance device product as protected information and must not use, communicate or publish it unless permitted by the Act.

The s37(2)(b), 37(1)(c), s47E(d) is solely responsible for storing and handling such product correctly.

Appointees must only use this protected information for lawful purposes including:

- lawful disclosure in proceedings in open court
- any purpose after lawful disclosure in open court
- where the appointee believes on reasonable grounds that using the information is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property
- communicating with the Australian Security Intelligence Organisation on matters relating, or appearing to relate, to activities prejudicial to security, within the meaning of the [Australian Security Intelligence Organisation Act 1979 \(Cth\)](#)
- communicating with a foreign country under the [Mutual Assistance in Criminal Matters Act 1987](#) (Cth)
- investigating a relevant offence within the meaning of this Act or a corresponding law
- deciding whether to prosecute a relevant offence
- keeping records and reporting under the Act
- an Ombudsman's inspection
- investigating under the [Privacy Act 1988](#) (Cth) or other law of a participating jurisdiction or

of the Commonwealth concerning the privacy of personal information.

13.3 Transcripts of foreign language product

When surveillance device product is wholly or partly in a foreign language, the case officer must ensure it is translated and transcribed into the English language as soon as possible. The original transcript, whether handwritten or typed, must be retained s37(2)(b), 37(1)(c), s47E(d).

The transcribed record must include:

- operation name
- warrant number
- time and date of translation
- interpreter's name
- typist's name (if typed) and the date typed.

14. Revocation of authorisation

When the circumstances surrounding the issue of surveillance device warrant change or no longer exist, case officers must advise s37(2)(b), 37(1)(c), s47E(d) of the changed circumstances and discuss whether to seek revocation of the authorisation.

When revocation of a warrant is requested the case officer must:

- ensure s37(1)(c), s47E(d) is advised so that the device is removed before the revocation of the warrant
- provide s37(2)(b), 37(1)(c), s47E(d) with sufficient details in writing of the reason for the revocation
- provide a Section 40 report to s37(2)(b), 37(1)(c), s47E(d) within 30 days after the revocation.

When a surveillance device is no longer to be used, investigators must immediately discuss with s37(1)(c), s47E(d) the issues regarding retrieving the device under the warrant provisions and before the warrant is revoked. This may negate the investigator's need to subsequently obtain a separate retrieval warrant to remove the device.

14.1 Surveillance device status when police on premises

Case officers should not, for accountability reasons, deactivate a surveillance device solely to prevent it from recording a police presence on the premises, such as a lawful premises search or an interview on the premises.

Exceptions to this rule include the device recovery procedures associated with expiration and revocation of the warrant.

15. Record keeping

Appointees must note that Division 5.3 of the *Crimes (Surveillance Devices) Act 2010* establishes the Ombudsman's inspection role. Appointees must comply with record-keeping provisions of the Act and related procedures in this guideline.

Appointees must bring to the attention s37(2)(b), 37(1)(c), s47E(d) any issues requiring legal advice or

review of this guideline.

15.1

s37(2)(b), 37(1)(c), s47E(d)

s37(2)(b), 37(1)(c), s47E(d)

15.2 Evidentiary certificates

The CPO or Deputy Chief Police Officer may sign and issue a certificate setting out any facts considered relevant to anything done by:

- an appointee, or a person assisting or providing technical expertise to the appointee, in order to execute a warrant or an emergency authorisation
- an appointee in relation to:
 - communication between persons
 - using, making or keeping records of information obtained with a surveillance device under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation.

This certificate is admissible as prima facie evidence of the matters stated in it. For emergency authorisations, the certificate is only admissible if the emergency authorisation is approved by a judge.

A pro forma evidentiary certificate is available from [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#). Each certificate must be:

- completed by the case officer
- quality assessed by their team leader
- forwarded via [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) to the authorised signatory.

16. Reporting

16.1 Reports to the minister

The [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) must prepare the annual written report to the minister per Section 38 of the *Crimes (Surveillance Devices) Act 2010* (ACT) and ensure it is delivered on time.

16.2 Final effectiveness report (Section 40 report)

The case officer must, within 30 days after a warrants ends, submit a final effectiveness report through their team leader [s37\(2\)\(b\), 37\(1\)\(c\), s47E\(d\)](#) on all surveillance device warrants issued to ACT Policing within their areas of responsibility.

Each final effectiveness report must relate to a single warrant and address:

- whether the warrant, or extension, amendment or revocation of a warrant was granted, refused or withdrawn
- warrant number
- date of issue
- period of validity
- expiry date
- name of the issuing judge or magistrate
- whether the warrant was executed.

If the warrant was **executed** the report must:

- state the:
 - name of each person involved in the execution of the warrant
 - kind of surveillance device used
 - period during which the device was used
 - name, if known, of any person whose conversations or activities were overheard, recorded, monitored, listened to or observed by the use of the device
 - name of the person, if known, whose geographical location was determined by the use of the device
- give details of:
 - any premises on which the device was installed or any place at which the device was used
 - any object in or on which the device was installed or any premises where the object was located when the device was installed
 - the communication of evidence or information obtained by the use of the device to persons other than officers of the agency
 - the use of information obtained by the use of the device by the agency, or by officers of the agency
 - each occasion when information obtained by the use of the device was given in evidence in a relevant proceeding
 - compliance with the conditions (if any) to which the warrant or authorisation was subject
 - if the warrant was issued in respect of the investigation of a relevant offence, the benefit to the investigation of the use of the device and of the general use made or to be made of any evidence or information obtained by the use of the device.

If the warrant was **extended or varied** the report must:

- give details of the number of extensions or amendments and the reasons for them.

In the case of an **emergency authorisation**, the report must:

- give details of the emergency authorisation (emergency use or continued use)
- state whether the application was granted, refused or withdrawn.

In the case of a **retrieval warrant**, the report must:

- give details of any premises entered, anything opened and any object removed and replaced under the warrant
- state whether the surveillance device was retrieved under the warrant
- if the device was not retrieved, state the reason(s) why
- give details of the compliance with the conditions (if any) to which the warrant was subject.

17. Further advice

Queries about the content of this guideline should be referred to the Superintendent Criminal Investigations.

18. References

Legislation

- [Australian Federal Police Act 1979](#) (Cth)
- [Australian Security Intelligence Organisation Act 1979](#) (Cth)
- [Crimes \(Surveillance Devices\) Act 2010](#) (ACT)
- [Mutual Assistance In Criminal Matters Act 1987](#) (Cth)
- [Privacy Act 1988](#) (Cth)
- [Surveillance Devices Act 2004](#) (Cth)
- [Telecommunications \(Interception and Access\) Act 1979](#) (Cth).

AFP governance instruments

- [AFP National Guideline on Surveillance Devices](#).