Australian Government

Australian Commission for Law Enforcement Integrity

STANDARD OPERATING PROCEDURE

SURVEILLANCE DEVICE WARRANTS

Australian Government
Australian Commission for Law Enforcement Integrity

Relevant Legislation and Other Links

- *Surveillance Devices Act 2004* (Cth) ('SD Act')
- *Telecommunications (Interception and Access) Act 1979* (Cth) ('TIA Act')
- *Crimes Act 1914* (Cth) – specifically the Integrity Testing provisions in Part 1ABA

This Standard Operating Procedure needs to be read in conjunction with the following Standard Operating Procedures:

- Telecommunication Intercepts
- Telecommunications Data Authorisations
- Controlled Operations and Integrity Testing

Previous Versions

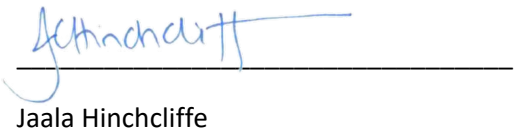
Version 1 – Effective date March 2010 – CM 13#5176DOC

Version 2 – Effective date October 2015 – CM 13#5177DOC

Version 3 – Effective date 23 March 2016 – CM 15#9193DOC

Approval

This Standard Operating Procedure is approved.



Jaala Hinchcliffe

Integrity Commissioner

16 August 2021

TEMPLATES

Warrants

Surveillance Device Warrants	
Decision Minute – Request for an SD warrant application	21#20952DOC
Application for an SD warrant – relevant offence/integrity operation	21#20951DOC
Affidavit for an SD warrant – relevant offence/integrity operation	21#20950DOC
Warrant – Surveillance Device	21#20949DOC
Application for an Extension/Variation – SD warrant	21#20948DOC
Affidavit for Extension – SD warrant	21#20947DOC
Affidavit for Variation – SD warrant	21#20946DOC
Decision Minute – Revocation – SD warrant	21#20945DOC
Computer Access Warrants	
Application – Computer Access Warrant – relevant offence/integrity operation	21#20944DOC
Affidavit – Computer Access Warrant – relevant offence	21#20943DOC
Affidavit – Computer Access Warrant – integrity operation	21#20942DOC
Warrant – Computer Access	21#20941DOC
Application for Extension/Variation – Computer Access Warrant	21#21080DOC
Affidavit for Extension – Computer Access Warrant	21#20940DOC
Affidavit for Variation – Computer Access Warrant	21#20939DOC
Decision Minute – Revocation – Computer Access Warrant	21#20938DOC
Retrieval Warrants	
Application – Retrieval Warrant	21#20937DOC
Affidavit – Retrieval Warrant	21#20936DOC
Warrant – Retrieval	21#20935DOC
Decision Minute – Revocation – Retrieval Warrant	21#20934DOC

Sharing Material

Communication of SD material – s45 Letter	21#20930DOC

Evidence and Destruction

Evidentiary certificate	21#20929DOC
Decision Minute – Section 46 – Retention of SD material	21#20924DOC
Decision Minute – Section 46 – Destruction of SD material	21#20923DOC

Reporting

Internal reporting Sheet – Section 45	21#20933DOC
Occurrence Log	21#20932DOC
Use and Communication Log – Section 45	21#20931DOC
Decision Minute – Section 49 report	21#20928DOC
Section 49 report	21#20927DOC
Section 49 report – Letter to Home Affairs	21#20926DOC
Section 49 report – warrant not executed	21#20925DOC

Australian Government
Australian Commission for Law Enforcement Integrity

CONTENTS

Australian Government
Australian Commission for Law Enforcement Integrity

1. INTRODUCTION

Purpose and background

1.1 The Parliament of Australia has provided the Integrity Commissioner and the Australian Commission for Law Enforcement Integrity (ACLEI) with sensitive, covert law enforcement powers. The use of these powers has the potential to affect privacy and other liberties of individuals.

1.2 To protect the legal rights of all parties, including ACLEI, this Standard Operating Procedure (SOP) aims to ensure that:

a) the use of surveillance devices is conducted in strict accordance with the law;

b) such operations are demonstrably fair; and

c) appropriate records are kept to meet transparency and accountability requirements.

1.3 The use of surveillance devices can provide important evidence in an ACLEI investigation, allowing investigators to collect information covertly on a target's movements and activities. However, the use of surveillance devices has the potential to interfere with an individual's privacy to a high degree and must be justified in every instance.

1.4 The SD Act creates a regime for the lawful collection of information by way of surveillance devices. It imposes a scheme of warrants, record keeping and reporting which ensures that the use of a surveillance device is measured and justified, and that material collected is managed securely to mitigate any privacy intrusions.

1.5 The SD Act also creates a general prohibition of the use, recording, communication or publication of protected information, obtained under an SD Act warrant, or its admission into evidence. Because of this, it is critical that the procedures set out in the SD Act are adhered to in order to ensure ACLEI staff members are acting within their legal authority, and that any material collected may be admissible as evidence.

2. DEFINITIONS

2.1 Key definitions are listed below. A full list of definitions is available at section 6 of the SD Act.

Appropriate authorising officer	The

	Integrity Commissioner, or a staff member of ACLEI who is an SES employee authorised by the Integrity Commissioner. See section 6A(4) of the SD Act.
Computer Access Warrant	A **computer access warrant** means a warrant issued under section 27C or subsection 35A(4) or (5).
Data surveillance device	A **data surveillance device** means any device or program capable of being used to record or monitor the input of information into, or the output of information from, an electronic device for storing or processing information, but does not include an optical surveillance device.
Enhancement equipment	**Enhancement equipment** in relation to a surveillance device, means equipment capable of enhancing a signal, image or other information obtained by the use of the surveillance device.
Issuing Authority	An eligible judge or a nominated member of the Administrative Appeals Tribunal (AAT) –see sections 12 and 13 of the SD Act.
Law enforcement officer	A **law enforcement officer** has the meaning given by subsection 6A(3). For ACLEI, a law enforcement officer is any staff member in the Operations branches at EL1, EL2 or SES level who have been authorised by the Integrity Commissioner under section 6B of the SD Act.
Listening device	A **listening device** means 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 does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear.
Optical surveillance device	An **optical surveillance device** means any device capable of being used to record visually or observe an activity, but does not include

	spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment
Protected information	As defined in section 44 of the SD Act.
Tracking device	A **tracking device** means any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object.
Relevant offence	A category of offence listed in section 6 of the SD Act, or prescribed by the SD regulations.
Retrieval warrant	A **retrieval warrant** means a warrant issued under Division 3 of Part 2 of the SD Act.
State or Territory relevant offence	A relevant offence against the law of a State or self-governing Territory that is punishable by a maximum term of imprisonment of 3 years or more or for life.
State or Territory relevant proceeding	As defined by subsection 45(9) of the SD Act, but can include: - the prosecution of a State or Territory relevant offence; or - a disciplinary offence against a public officer.
Surveillance device warrant	A **surveillance device warrant** means a warrant issued under Division 2 of Part 2 or under subsection 35(4) or (5) of the SD Act.
Target agency	A **target agency** means any of the following: (a) the Australian Federal Police; (b) the Australian Crime Commission; (c) the Immigration and Border Protection Department.

Target computer	A **target computer** means: (a) a particular computer; (b) a computer on particular premises; (c) a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known). See s 27A(15) of the SD Act

3. ROLES AND RESPONSIBILITIES

Case officer	The case officer is responsible for preparing the request for an SD warrant application and ensuring the relevant Director Operations has the information required in order for them to decide whether it is appropriate to proceed with SD warrant application. If the Director Operations decides there is sufficient material to make an application, they will then determine who the most appropriate 'law enforcement officer' is to make that application. Generally this will be the either Director Operations themselves or the case officer. The case officer must then create the appropriate folder structure in CM, draft all the relevant documents, and save all the draft documents into the relevant folders. After the warrant is issued, the case officer is responsible for saving the signed documents into the relevant CM folders, and providing the authorised paperwork to the Operational Support Team for storage production to the Ombudsman as required. The case officer is responsible for liaising with the assisting agency and facilitating access to the Protected material that is collected. The case officer is also responsible for ensuring the material being collected is within the scope and authority of the warrant.

	The case officer is responsible for ensuring all action sheets from assisting agencies are received and saved into the relevant CM folders. The case officer is responsible for recording any use or disclosure of the material provided under warrant in the Use and Disclose log. The case officer is responsible for completing the Internal Warrant Report at the cessation of the warrant. The case officer must be available during inspections by the Ombudsman's office to discuss any warrants issued. The case officer is responsible for arranging the destruction of material at the conclusion of the investigation.
Director Operations	The relevant Director Operations is ultimately responsible for considering requests for SD warrants against the criteria set out in the SD Act. If the Director Operations is satisfied an SD warrant application is appropriate, they will then determine the most appropriate law enforcement officer to make the application. The Director Operations must review all application and affidavit paperwork prior to the application being made to the issuing authority. The Director Operations will make themselves available during inspections by the Ombudsman to discuss any warrants for which they are responsible.
Operational Support Team	The Operational Support Team can provide assistance to the case officer in relation to requesting SD warrants. It is best practice for the case officer to liaise with the Operational Support team prior to making a request for an SD warrant.

	The Operational Support Team is responsible for: a) Processing warrants; b) Assisting with any device monitoring requirements; c) Ensuring revocation paperwork is issued as necessary; d) Preparing reports required under the SD Act; and e) Liaising with the Ombudsman in relation to inspections.

4. WHAT IS A SURVEILLANCE DEVICE

4.1 A surveillance device is defined as:

a) A data surveillance device – a device or program that records or monitors computer inputs and outputs; or

b) A listening device – a device which allows for the listening to, recording of or monitoring of persons conversation; or

c) An optical device – a device which enables the visual recording or observation of an activity; or

d) A tracking device – a device which is used to determine or monitor the location of a person or object; or

e) A device that combines any two or more of the above items – for example, a camera which records both audio and video is both a listening device and an optical device.

5. WHO CAN APPLY FOR A SURVEILLANCE DEVICE WARRANT

5.1 SD warrants may only be applied for by a 'law enforcement officer'. For the purposes of section 6B of the SD Act, ACLEI 'law enforcement officers' are the Integrity Commissioner and those officers within the Operations Northern and Southern branches at the classification level of SES, EL2 or EL1. For the purpose of this SOP, these officers will be referred to as 'the applicant'. The relevant Director Operations will determine the most appropriate law enforcement officer to apply for the SD warrant on a case by case basis.[1]

[1] Section 6B of the SD Act

5.2 Current ACLEI authorisations relevant to the SD Act can be found on the intranet.

6. WHO CAN ISSUE A SURVEILLANCE DEVICE WARRANT

6.1 An SD warrant can be issued by an 'eligible judge' or 'nominated AAT member', as defined in sections 12 and 13 respectively of the SD Act.

6.2 The AAT acts as an initial point of contact for both AAT members and Federal Circuit Court Judges who can issue surveillance device warrants. The local registry contact numbers for the AAT are:

a) Canberra: (02) 6243 4611

b) Sydney: (02) 9391 2400

6.3 Throughout this SOP the term 'issuing authority' is used to refer to an eligible judge or nominated AAT member.

7. WHAT ARE THE TYPES OF SURVEILLANCE DEVICE WARRANTS

7.1 There are a number of types of warrants which an ACLEI officers may apply for under the SD Act, including:[2]

a) a surveillance device warrant;

b) a computer access warrant; and

c) a retrieval warrant.

7.2 While there are a number of reasons that an application for a warrant under the SD Act may be made, the main reasons an ACLEI officer will apply is:

a) for the investigation of a relevant offence; or

b) the conduct of an integrity testing operation; or

c) the retrieval of lawfully installed devices.

[2] Section 10 of the SD Act

8. SURVEILLANCE DEVICE WARRANTS

What an SD Warrant authorises[3]

8.1 A surveillance device warrant allows for the installation, use and maintenance of one or more of the surveillance devices listed above to be used during the investigation of a 'relevant offence', or for the purpose of an integrity testing operation or integrity testing controlled operation. A 'relevant offence' includes a Commonwealth offence or a State offence with a Federal aspect, punishable upon conviction by a minimum of three years.[4]

8.2 For ACLEI investigations, technical assistance in the installation, maintenance and retrieval of surveillance devices will be provided by partner agencies. This is discussed in more detail below.

8.3 Ideally, attempts should be made to retrieve all SD devices and associated equipment prior to the SD warrant expiring, to avoid having to apply for a retrieval warrant. In circumstances where this is not possible, a retrieval warrant will be required.

8.4 Of note:

a) An SD warrant can only be issued for a period of no more than 90 days; or

b) If the warrant is issued for the purposes of an Integrity operation, a period of no more than 21 days.[5]

SD Warrants sought for offence investigations

8.5 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:

a) one or more relevant offences have been, are being, are about to be, or are likely to be, committed;

b) an investigation into those offences is being, will be, or is likely to be, conducted; and

c) the use of a surveillance device is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of the commission of the relevant offences or the identity or location of the offenders.

[3] Section 18 of the SD Act
[4] Section 6(1) of the SD Act
[5] Section 18 of the SD Act

SD Warrants sought for integrity operations

8.6 If the SD warrant is being sought in support of an integrity testing operation, there must be:

a) an integrity testing authority in effect authorising an integrity operation in relation to an offence that is suspected has been, is being or is likely to be committed by a staff member of a target agency; and

b) the applicant must suspect on reasonable grounds that the use of a surveillance device will assist in the conduct of the integrity operation by:

(i) recording or monitoring the operation; and

(ii) enabling evidence to be obtained relating to the commission of the offence or the integrity, location or identity of any staff member of the target agency.

8.7 Further information about the application process is detailed below.

9. COMPUTER ACCESS WARRANTS[6]

Warrants sought for offence investigations

9.1 Computer access warrants can be applied for if the applicant suspects on reasonable grounds that:

a) one or more relevant offences have been, are being, are about to be, or are likely to be, committed;

b) an investigation into those offences is being, will be, or is likely to be, conducted; and

c) access to data held in a computer (the target computer) is necessary, in the course of that investigation, for the purpose of enabling evidence to be obtained of:

(i) the commission of those offences; or

(ii) the identity or location of the offenders.

[6] Section 27A and 27E of the SD Act

Warrants sought for integrity operations

9.2 If a computer access warrant is being sought in support of an integrity operation, the application can only be made if:

a) an integrity authority is in effect authorising an integrity operation in relation to an offence suspected to have been committed, being committed or is likely to be committed by a staff member of a target agency; and

b) the law enforcement officer suspects on reasonable grounds that access to data held in a computer (**the target computer**) will assist the conduct of the integrity operation by enabling evidence to be obtained relating to the integrity, location or identity of any staff member of the target agency.

9.3 Further information about the application process is detailed below, and the relevant *AFP Better Practice Guide* provides further information on the use of computer access warrants.

10. RETRIEVAL WARRANTS[7]

10.1 A retrieval warrant may be applied for to retrieve a device that was installed under the authority of a surveillance device warrant, if the applicant suspects on reasonable grounds the device remains in situ.

10.2 Urgent applications and remote applications (telephone, fax, email etc.) can be made, usually in order to retrieve a device that is at risk of detection, in order to protect law enforcement methodology. In the case of ACLEI investigations these situations are rare and advice from support agency technicians about the urgency of the retrieval should always be taken and considered.

10.3 A retrieval warrant will allow:

a) the retrieval of the surveillance device specified in the warrant and any enhancement equipment in relation to the device;

b) the entry, by force if necessary, onto the premises where the surveillance device is reasonably believed to be, and onto other premises adjoining or providing access to those premises, for the purpose of retrieving the device and equipment;

c) the breaking open of any thing for the purpose of retrieving the device and equipment;

[7] Section 22 of the SD Act

d) if the device or equipment is installed on or in an object or vehicle—the temporary removal of the object or vehicle from any place where it is situated for the purpose of retrieving the device and equipment and returning the object or vehicle to that place; and

e) the provision of assistance or technical expertise to the law enforcement officer named in the warrant in the retrieval of the device or equipment.

11. CONSIDERATIONS BY THE ISSUING AUTHORITY

Considerations in relation to SD Warrants[8]

11.1 Section 16 of the SD Act lays out the considerations an issuing authority must be satisfied with before they issue an SD warrant. These considerations vary, depending on which type of SD warrant application is being made by the law enforcement officer (eg. In support of the investigation of a relevant offence, in support of an Integrity testing operation etc). These considerations are complex, and should be reviewed prior to submitting any application, to ensure the application is able to satisfy each consideration.

Considerations in relation to Retrieval Warrants[9]

11.2 The issuing authority may issue a retrieval warrant if they are satisfied:

a) that there are reasonable grounds for the suspicion founding the application for the warrant; and

b) in the case of an unsworn application—that it would have been impracticable for an affidavit to have been sworn or prepared before the application was made; and

c) in the case of a remote application—that it would have been impracticable for the application to have been made in person.

11.3 The issuing authority must also consider:

a) the extent to which the privacy of any person is likely to be affected; and

b) the public interest in retrieving the device sought to be retrieved.

11.4 It is essential that any application for a retrieval warrant addresses these considerations in order to contribute to the success of the application.

[8] Section 16 of the SD Act
[9] Section 24 of the SD Act

Considerations in relation to Computer Access Warrants

11.5 An issuing authority may issue a computer access warrant if they are satisfied:

a) in the case of a warrant sought in relation to a relevant offence –

(i) that there are reasonable grounds for the suspicion founding the application for the warrant;[10] and

b) in the case of a warrant sought for the purposes of an integrity operation –

(i) that an integrity authority is in effect authorising an integrity operation in relation to an offence that it is suspected has been, is being, or is likely to be committed by a staff member of a target agency; and

(ii) the applicant suspects on reasonable grounds that access to data held on the target computer will assist the conduct of the integrity operation by enabling evidence to be obtained relating to the integrity, location or identity of any staff member of the target agency.[11]

11.6 In addition, when considering a computer access warrant in support of the investigation of a relevant offence or an integrity testing operation, the issuing authority must have regard to:

a) the nature and gravity of the alleged offence;

b) the extent to which the privacy of any person is likely to be affected;

c) the existence of any alternative means of obtaining the evidence or information sought to be obtained;

d) the likely evidentiary or intelligence value of any evidence or information sought to be obtained; and

e) any previous warrant sought or issued under Division 4 of the SD Act in connection with the same alleged offence.

11.7 It is essential that any application for a computer access warrant addresses these considerations in order to contribute to the success of the application.

[10] Subsection 27C(1)(a) of the SD Act
[11] Subsection 27C(1)(d) of the SD Act

12. APPLYING FOR A WARRANT

12.1 Prior to making an application for a warrant under the SD Act, the case officer must discuss the proposed course of action with the relevant Director Operations in the first instance.

12.2 Following advice from the relevant Director Operations as to the most appropriate warrant and most applicable type of surveillance device(s) for the situation, the case officer will create a new CM folder within the investigation container to record all documentation relating to the application. Within this folder, case file dividers must then be created for each separate warrant being applied for, where documentation and correspondence about the relevant warrant(s) must be saved.

12.3 The case officer must then complete a Decision Minute to the relevant Director Operations, justifying why the particular warrant is being sought and detailing how it will advance the investigation. The Decision Minute should satisfy each of the applicable tests in the SD Act[12] and should include the following information:

a) Name of the applicant;

b) The type of surveillance warrant being sought (SD warrant, computer access warrant or Retrieval warrant);

c) The type of surveillance devices sought;

d) The target of the surveillance device/s (person, premises, vehicle, object etc);

e) Duration of the warrant sought; and

f) The use of a surveillance device is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of the commission of the relevant offences or the identity or location of the offenders.

12.4 If the case officer does not satisfy Director Operations that the tests in the SD Act have been made out, then the application will not be supported and no approval will be granted to make the application.

12.5 Alternatively, if the Director Operations *is* satisfied that each of the applicable tests in the SD Act have been made out and that it is appropriate to apply for a SD warrant, they will endorse the recommendation in the Decision Minute and provide approval to proceed with the warrant application.

[12] Sections 14 and 16 of the SD Act

12.6 If this Decision Minute is supported by Director Operations, the case officer will then draft all the relevant paperwork, including an affidavit, applications and warrants. While the affidavit can support multiple warrant applications, a separate application and warrant document must be drafted **for each warrant** being sought.

12.7 The Director Operations will determine who the most appropriate law enforcement officer is to make the application (see 'Who can apply for an SD warrant' above).

12.8 The law enforcement officer making the application must review the draft warrant and supporting affidavit and ensure that the information included is correct and sufficient to enable the issuing authority to make a decision on issuing the warrant. Any changes to the draft paperwork must be made prior to the affidavit being sworn.

12.9 There are several areas of the warrant template which can be struck through if not applicable. The sections on conditions and restrictions should be left with sufficient space for the issuing authority to add conditions or restrictions if they elect to do so. If the issuing authority does not make any conditions or restrictions, they should either strike through that section of the warrant or indicate on the warrant that those sections are not applicable.

12.10 An ACLEI staff member with access to the AFP Net can assist in ensuring that the end date for the warrant is correctly calculated, by utilising the AFP Warrant Date Calculator – **AFP Hub > Operational info and resources > Investigators Toolkit > Special projects > Warrant date calculator**.

12.11 When an application for an SD warrant is being considered, the case officer and Director Operations must engage with ACLEI Legal at the earliest opportunity. ACLEI Legal should be given the opportunity to review all applications, if practicable to do so, prior to the application being made. If formal legal advice is required, the process for requesting the advice is available on the intranet.

12.12 Once the draft affidavit, application and warrant is approved by Director Operations, the affidavit needs to be sworn by the law enforcement officer making the application. ACLEI Legal can assist with this.

13. APPEARING BEFORE THE ISSUING AUTHORITY

13.1 Once the affidavit is sworn, the case officer will need to make an appointment with an issuing authority for the application to be formally made. The Operational Support team can assist with making this appointment. The sworn affidavit and draft paperwork should be provided to the issuing authority for consideration.

13.2 The issuing authority may decide whether to issue the warrant based on the affidavit or may require the applicant and/or case officer to provide further oral evidence on oath or affirmation.

13.3 If the issuing authority decided to grant the warrant(s), they will sign, date and note the time on the warrant itself and initial each page of the warrant. They may also initial the affidavit. The warrant and affidavit will then be returned to the applicant.

Following the warrant being issued

13.4 The case officer must save scanned copies of all issued and/or sworn documents into the relevant CM folders and provide all original documentation to the Operational Support team, regardless of whether the warrant was issued or not.[13]

13.5 It is also the responsibility of the case officer to ensure all documentation and correspondence relating to material captured under the SD warrants is stored in the relevant CM case file divider, not in other investigation folders within CM. This will ensure a centralised location of material for subsequent destruction at the end of the investigation.

14. REMOTE APPLICATIONS

14.1 The SD Act provides for warrant applications to be made by telephone, fax, email or any other form of communication, if the applicant believes it is impractical for an application to be made in person.[14]

14.2 In these circumstances, the information to be given to the issuing authority is the same as would be required in a written application, with the addition of the circumstances that the person making the application thinks makes it impractical to make the application in person.

14.3 If fax transmission is possible, and an affidavit in support of the application has been prepared, whether sworn or unsworn, a copy of the affidavit must be provided via fax to the issuing authority for consideration.[15]

14.4 It would be only in very rare circumstances that an ACLEI SD warrant application would be made by any method other than in person to the issuing authority. Any consideration of a remote application must be discussed with the relevant Director Operations in the first instance.

---

[13] Note: For Sydney base staff, original warrant paperwork will be retained by the relevant Director Operations if the warrant needs to be extended. Once the warrant has ceased to be in force, all original paperwork can be safe hand delivered to Canberra and added to the warrant file.
[14] Sections 15, 23 and 27B of the SD Act
[15] Subsections 15(2), 23(2) and 27B(2) of the SD Act

15. MONITORING SURVEILLANCE DEVICES

Resource allocation and monitoring arrangements

15.1 Depending on the surveillance device in use and arrangements in place with the assisting agency, it may be possible for surveillance devices to be monitored by ACLEI staff in Canberra and/or Sydney. On other occasions, ACLEI staff may need to deploy into the assisting agency's location, or the assisting agency may provide monitoring staff and share material with ACLEI.

15.2 The allocation and use of ACLEI and assisting agency resources will be managed on a case by case basis. Decisions around resourcing of surveillance devices will be made by the Operations Board in consultation with the case officer. Assistance from the Director Operations and Executive Director Operations may be required to gain assisting agency resources and support.

15.3 Day to day monitoring duties can be managed between the Director Operations and Director Assessments and Operational Support. Any issues arising can be discussed at the next scheduled Operations Board meeting as required.

Legal professional privilege and SD material

15.4 ACLEI staff involved in SD monitoring must be alert to the likelihood that SD material may involve communications with a legal practitioner, especially if he or she has had dealings with ACLEI or another agency (through being interviewed, served with a summons, served with a coercive notice, arrested or been subject to a search warrant). These communications are likely to be subject to a claim of legal professional privilege (LPP).

15.5 Privilege 'belongs' to the client, not the legal practitioner. The client may waive privilege by disclosing the advice to another person or doing something inconsistent with maintaining the privilege. If matters of this nature arise, ACLEI Legal should be consulted at the earliest opportunity and advice sought as necessary.

15.6 Where a monitor or other ACLEI staff member becomes aware that SD material contains communication between a target and a legal practitioner, the monitor must cease listening and inform the case officer and Director Operations. ACLEI Legal should also be advised and advice sought if necessary. The Director Operations, following advice as required, will then consider the specific situation, in particular:

a) whether the communication is likely to subject to a claim of LPP;

b) whether an exception or qualification to LPP exists and whether a waiver has potentially occurred; and

c) the steps ACLEI should take in the circumstances, including quarantining of the material.

15.7 ACLEI staff should seek advice from ACLEI Legal if they are considering obtaining or executing a warrant under the SD Act which will affect a legal practitioner.

15.8 If a law enforcement agency is known to have become aware of the content of privileged communications in the course of an investigation and does not take appropriate steps to quarantine this information from the investigation, it may compromise future prosecutions arising from that investigation.

16. EMERGENCY AUTHORISATIONS

16.1 Part 3 of the SD Act defines the basis for an emergency authorisation for the use of a surveillance device or emergency access to data held on a target computer.

16.2 For emergency use of a surveillance device, the applicant must reasonably suspect that:[16]

a) an imminent risk of serious violence to a person or substantial damage to property exists; and

b) the use of a surveillance device is immediately necessary for the purpose of dealing with that risk; and

c) the circumstances are so serious and the matter is of such urgency that the use of a surveillance device is warranted; and

d) it is not practicable in the circumstances.

16.3 For emergency authorisation for access to data held in a target computer, the applicant must reasonably suspect that:[17]

a) an imminent risk of serious violence to a person or substantial damage to property exists; and

b) access to data held in the target computer is immediately necessary for the purpose of dealing with that risk; and

c) the circumstances are so serious and the matter is of such urgency that access to data held in the target computer is warranted; and

d) it is not practicable in the circumstances to apply for a computer access warrant.

[16] Subsection 28(1) and 28(1A) of the SD Act
[17] Subsection 28(1) and 28(1A) of the SD Act

16.4 It is unlikely that an ACLEI investigation will require the use of an emergency authorisation. However, if the circumstances arise, the relevant Director Operations and Executive Director Operations must be consulted in the first instance as a matter of urgency.

17. DURATION OF A WARRANT

17.1 An SD warrant and a Computer Access Warrant can be in force for a maximum period of up to 90 days, except if the warrant is applied for as part of an integrity testing authority and in support of an integrity operation, in which case it can only be in force for a maximum of 21 days.[18] A retrieval warrant can be in force for a maximum period of 90 days.[19]

17.2 Any ACLEI staff member with access to the AFPNet can assist in ensuring that the end date for the warrant is correctly calculated by using the AFP Warrant Date Calculator – **AFP Hub > Operational info and resources > Investigators Toolkit > Special projects > Warrant date calculator**).

17.3 An SD warrant and Computer Access Warrant can be extended by way of an application to an issuing authority at any time before the warrant expires.[20] The warrant cannot be extended for more than a maximum period of 90 days, except if the warrant is applied for on the basis of an integrity testing authority and in support of an integrity operation, in which case it cannot be extended for more than a maximum period of 21 days. The original warrant will need to be provided to the issuing authority for endorsement of the extension period.

17.4 Retrieval warrants cannot be extended; however, there is no restriction on the number of successive warrants that can be issued. A subsequent retrieval warrant would need to be applied for if necessary (detailed further below).

17.5 It is desirable for investigators to have ongoing and uninterrupted access to SD material. For this reason it is obviously important to avoid a situation arising where retrieval and reinstallation of surveillances devices occurs during an investigation. To ensure this does not occur, in cases where an extension likely to be sought the case officer must draft all documentation for review and approval prior to the SD or Computer Access Warrant expiring.

[18] Subsection 17(1A) of the SD Act
[19] Subsection 25(1)(b)(v) of the SD Act
[20] Section 19 and 27F of the SD Act

18. REVOCATION

SD Warrant

18.1 If the Integrity Commissioner is satisfied that that the use of a surveillance device under authority of the warrant is no longer necessary for the purpose of obtaining evidence of the commission of the relevant offence or the identity or location of the offender, then he or she must, in addition to revoking the warrant under section 20 of the SD Act, take the steps necessary to ensure that use of the surveillance device authorised by the warrant is discontinued.

18.2 In the case of a warrant sought under an integrity testing authority in support of an integrity operation, if the integrity testing authority for the integrity operation is no longer in force, the Integrity Commissioner must, in addition to revoking the warrant, take the steps necessary to ensure that use of the surveillance device authorised by the warrant is discontinued

18.3 If a case officer forms the view that the grounds for issuing the warrant cease to exist, they must inform the Integrity Commissioner immediately and recommend the Integrity Commissioner revoke the warrant. It is the case officer's responsibility to draft the relevant revocation paperwork for the Integrity Commissioner to consider.

18.4 The case officer should ensure that all devices are retrieved prior to the warrant being revoked. If this is not possible, the case officer must ensure all devices are disabled, to ensure no recording is undertaken after the revocation is authorised. The case officer will then need to apply for a retrieval warrant to retrieve the devices at a later date.

Computer Access Warrant

18.5 If the Integrity Commissioner is satisfied that that access to data under the warrant is no longer required for the purpose of enabling evidence to be obtained of the commission of the relevant offence, or the identity or location of the offender, the integrity Commissioner must, in addition to revoking the warrant under section 27G of the SD Act, take the steps necessary to ensure that access to data authorised by the warrant is discontinued.

18.6 In the case of a warrant sought under an integrity testing authority in support of an integrity operation, if the integrity testing authority for the integrity operation is no longer in force, the Integrity Commissioner must, in addition to revoking the warrant, take the steps necessary to ensure that access to data authorised by the warrant is discontinued.

18.7 If a case officer forms the view that access to data under the warrant is no longer necessary, or that the integrity authority for the integrity operation is no longer in force, they must inform the Integrity Commissioner immediately and recommend the Integrity Commissioner revoke the warrant. It is the case officer's responsibility to draft the relevant revocation paperwork for the Integrity Commissioner to consider.

Retrieval Warrant[21]

18.8 If the case officer believes that the grounds for issue of the warrant no longer exist, he or she must inform the Integrity Commissioner immediately. It is the case officer's responsibility to draft the relevant revocation paperwork for the Integrity Commissioner to consider.

18.9 If the Integrity Commissioner is satisfied that the grounds for issue of the retrieval warrant no longer exist—he or she must, by instrument in writing, revoke the warrant.

18.10 The most common reason for the grounds of a retrieval warrant no longer existing, is in the case where all the devices have been retrieved under the warrant.

19. USE OF CERTAIN SURVEILLANCE DEVICES WITHOUT A WARRANT[22]

19.1 The SD Act allows for certain circumstances under which a surveillance device may be used without a warrant. Generally, ACLEI officers are not authorised to use a surveillance device without a warrant. If this is genuinely considered as a viable investigative option by the case officer, it should be discussed with relevant Director Operations and the relevant Executive Director Operations in the first instance.

Optical devices[23]

19.2 The most applicable circumstance where this might occur during an ACLEI investigation is use of an optical device for purposes linked to the functions of the Integrity Commissioner, and in situations that do not involve entry onto premises without permission or interference without permission with any vehicle or thing. In other words, the devices are installed in a public place such as a power pole, a street light or a tree.

Use of surveillance devices for listening to or recording words[24]

[21] Section 27 of the SD Act
[22] Part 4 of the SD Act
[23] Section 37 of the SD Act
[24] Section 38 of the SD Act

19.3 A listening device may be used in circumstances linked to the function of the Integrity Commissioner, and in situations where the law enforcement officer is the speaker of the words or is a person, or is included in a class or group of persons, by whom the speaker of the words intends, or should reasonably expect, the words to be heard; or the law enforcement officer listens to or records the words with the consent, express or implied, of a person who is permitted by one of those persons to listen to or record the words.

Use and retrieval of tracking devices – tracking device authorisations[25]

19.4 A law enforcement officer may, with the written permission of an appropriate authorising officer, use a tracking device without a warrant in the investigation of a relevant offence or for the purpose of an integrity operation. This written approval is known as a **tracking device authorisation**. The authorisation may authorise the use of more than one tracking device, and may authorise the retrieval of the device/s to which the authorisation relates.

19.5 A tracking device authorisation can only be inforce for a maximum period of 90 days, and the authority must state the period for which it remains in force.

19.6 An application, addressing the criteria of a surveillance device application, must be made orally or in writing to the appropriate authorising officer. If a tracking device authorisation is given by the Integrity Commissioner, it must address the material identified in section 40 of the SD Act.

19.7 An appropriate authorising officer must not give permission under this section for the use, installation or retrieval of a tracking device if the installation of the device, or its retrieval, involves entry onto premises without permission or an interference with the interior of a vehicle without permission.

19.8 If the case officer believes the use of a tracking device would be beneficial to the investigation, a discussion with the relevant Director Operations should occur to determine whether an SD Warrant or a tracking device authorisation is the most appropriate option.

20. USE AND DISCLOSURE

20.1 Material captured by surveillance devices under the SD Act is defined as 'protected information'. [26] There is a general prohibition on the use, recording, communication or publication of protected information, or its admission into evidence.

20.2 There are some exceptions to this prohibition, including but not limited to instances where:

[25] Section 39 of the SD Act
[26] Section 44 of the SD Act

a) the use, recording, communication or publication of any information that has been disclosed in proceedings in open court lawfully;

b) the use or communication of protected information by a person who believes on reasonable grounds that the use or communication is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property

c) the investigation of a relevant offence or the making of a report on the outcome of such an investigation;

d) the making of a decision whether or not to bring a prosecution for a relevant offence;

e) a relevant proceeding;

f) an investigation of a complaint against, or into the conduct of, a public officer within the meaning of the SD Act and also any subsequent investigation or prosecution of a relevant offence arising directly from the investigation of the complaint, or into the conduct; and

g) the making of a decision in relation to the appointment, term of appointment, termination of the appointment, or retirement, of a public officer within the meaning of the SD Act.

20.3 Full details of the exceptions to the general disclosure prohibition are detailed in section 45 of the SD Act, and should be reviewed carefully by the case officer prior to any use, recording, communication or publication of any protected information occurring. If in doubt, seek advice from the Operational Support Team, Director Operations and/or ACLEI Legal as necessary.

20.4 There are no special rules for joint task forces or joint ACLEI operations – the material needs to satisfy the general requirements for sharing or dealing. In order to ensure that any use or disclosure of information is done for a proper purpose, the SD Act requires the Integrity Commissioner to keep records of use and communication of SD product.

20.5 The case officer must maintain a Use and Disclosure log to record any use or disclosure of SD protected information. Any use of the SD material, including in internal documents such as the Final Investigation Report, must be recorded in this log and made available for auditing purposes and inspections by the Commonwealth Ombudsman.

20.6 The case officer must also ensure any agency assisting ACLEI are aware of their record keeping obligations in relation to protected information obtained from the use of an ACLEI issued SD warrant and ensure records are obtained and made available for the Commonwealth Ombudsman inspection. An email outlining record keeping obligations to the assisting agency should be sent to the assisting agency, and saved into CM for record keeping purposes.

Protected information in relation to Integrity Operations[27]

20.7 Protected information may be used, recorded, communicated or published, or may be admitted in evidence, if it is necessary to do so for any of the following purposes:

a) making a decision about whether to apply for an integrity authority;

b) designing an integrity operation;

c) applying for an integrity authority;

d) granting an integrity authority;

e) conducting an integrity operation;

f) applying for any warrant, authorisation or order, under a law of the Commonwealth, for the purposes of an integrity operation; and

g) any disciplinary or legal action in relation to a staff member of a target agency, if arising out of, or otherwise related to, an integrity testing operation.

21. EVIDENTIARY CERTIFICATES

21.1 The SD Act provides for the issuing of evidentiary certificates by the Integrity Commissioner, or an appropriate authorising officer. The effect of a certificate is to provide prima facie evidence of the protected information which the certificate deals with. There are certain restrictions and limitations on the admissibility of the certificate, which the case officer must be familiar with, in the case that a brief of evidence is required.[28] The Operational Support Team will assist in facilitating requests for evidentiary certificates. Of note, the person signing the certificate may be called to provide evidence, and may be made available for cross-examination. This should be carefully considered when the Integrity Commissioner is the signatory.

22. RECORD KEEPING

Keeping SD material

[27] Section 45A of the SD Act
[28] Section 62 of the SD Act

22.1 The SD Act outlines a number of documents and records that the Integrity Commissioner must keep.[29] In addition, the Integrity Commissioner must keep a register of warrants, emergency authorisations and tracking device authorisations sought by ACLEI officers, whether or not those warrants and authorities were granted.

22.2 It is the case officer's responsibility to complete an Internal SD report at the cessation of the warrant, and forward the completed report to the Operational Support team. The case officer must also maintain a Record Keeping Log during the conduct of the investigation, to ensure ACLEI's record keeping requirements are maintained. The Operational Support team is responsible for maintaining all original documents associated with SD Warrants obtained by ACLEI officers, and to co-ordinate ACLEI's reporting obligations under the SD Act.

Storage and Destruction of material

22.3 The SD Act stipulates that reports containing protected information must be maintained and stored in a secure place not accessible to people who are not entitled to deal with the record or report. The SD Act also stipulates when protected information must be destroyed.[30] Some of those circumstances include when the Integrity Commissioner is satisfied that the record or report:

a) Will not be relevant for a civil or criminal proceeding which has, or is likely to commence;

b) Is not likely to be required for a permitted use or dealing; and

c) Has been available for the ombudsman to inspect in a previous inspection.

22.4 Alternatively, the Integrity Commissioner must ensure protected records are destroyed within five years of the protected record being made[31]. The destruction of SD material must be approved by the Integrity Commissioner in a Decision Minute.

22.5 The case officer is responsible for ensuring the retention / destruction of protected material occurs once the investigation is finalised, and all associated reporting obligations and court proceedings are complete.

[29] Section 51 and 52 of the SD Act
[30] Section 46 of the SD Act.
[31] Subsection 46(b)(ii) of the SD Act

22.6 An exception to this is that the Integrity Commissioner does not need to destroy the material if he or she is satisfied that the material may be required for a circumstance listed above after the 5 year period. In such a case, the case officer should prepare a Decision Minute before the 5 year period expires, recommending the material be retained. This process must be repeated every 5 years, but the status of the protected information may be reviewed prior to the 5 year period expiring.

22.7 These obligations do not apply to a record or report that has been received into evidence in legal or disciplinary proceedings.[32]

22.8 Once approval has been granted for the protected information to be destroyed, the case officer must provide a catalogue of CM files that need to be destroyed to the ACLEI IT team, who will arrange for those files to be deleted from CM by a CM Administrator at the Attorney General's Department. The decision minute approval must also be saved into the relevant SD material case file dividers. The case officer must also ensure that SD material held by other supporting agencies is also destroyed at the same time.

23. RECORD KEEPING, REPORTING AND AUDIT

Reports to the Minister for each warrant

23.1 The Integrity Commissioner must make a report to the Minister for Home Affairs in relation to each warrant, emergency authorisation or tracking device authorisation issued to ACLEI (including those issued to staff seconded to ACLEI).[33] The Operational Support Team are responsible for ensuring these reports are made to the Minister. A Decision Minute should be prepared seeking the Integrity Commissioner's approval to make the report to the Minister. Once approved, the report can then be sent, accompanied by a letter to the Attorney-General's Department.

23.2 The report must be made as soon as practicable after the warrant or authorisation ceases to be in force. It is ACLEI's policy that the report should be forwarded no more than three months after the cessation of the warrant or authorisation.

23.3 A copy of each warrant or authorisation, and any instrument revoking, extending or varying them must be attached to the report.

23.4 Section 49(2) of the SD Act details the information that must be provided in the report in the case of an SD warrant or authorisation and s 49(3) details the information that must be provided in the report in the case of a retrieval warrant. The report must include:

---

[32] Section 46(3) of the SD Act
[33] Section 49 SD Act.

a) the name of the executing officer;

b) the name of each person responsible for the installation, maintenance and retrieval of each device used under the warrant or authorisation;

c) the kind of surveillance device/s used;

d) the period during which the device/s was used;

e) the names of any person whose conversations or activities were listened to, recorded, overheard, monitored or observed by the use of the device;

f) the name of any person whose location was determined by the use of a tracking device;

g) details of any premises, place or object where the device/s was installed or used;

h) the details of the benefit to the investigation or integrity operation of the use of the device/s;

i) the general use made or communication of the information obtained by the use of the device/s; and

j) if applicable, the number of times the warrant was extended or varied, and the reasons for this.

Annual report to the Minister

23.5 The Integrity Commissioner must submit a report on the use of SD warrants to the Minister as soon as practicable after the end of the financial year. This report must be submitted within three months after the end of the financial year. The Operational Support team is responsible for drafting this report and submitting it to the Integrity Commissioner.[34]

Inspections by the Commonwealth Ombudsman[35]

23.6 The Commonwealth Ombudsman is required to inspect ACLEI's records to determine the extent of ACLEI's compliance with the SD Act. The Ombudsman has extensive powers to enter premises and examine records.

[34] Section 50 of the SD Act details what must be included in the annual report.
[35] Division 3 of the SD Act

23.7 Consequently personnel from the Commonwealth Ombudsman office will attend ACLEI periodically to inspect the records. The Ombudsman's staff should have unrestricted access to ACLEI's records related to SD warrants. ACLEI staff must provide the Ombudsman's inspectors with all necessary assistance to enable them to perform their duties.

23.8 The Operational Support team will facilitate any visit by the Commonwealth Ombudsman for the purpose of record inspection.

23.9 Case officers who have utilised SD warrants in their investigations, and the relevant Director Operations overseeing those investigations during the inspection period must make themselves available to inspectors at any time during an inspection as necessary.