# Victoria Police Manual – Policy Rules

## Investigation support

### Context

Victoria Police can use a number of covert methods to gather evidence and intelligence when conducting an investigation. These include:

- covert physical surveillance
- undercover operatives
- surveillance devices
- telecommunications interceptions
- controlled operations
- assumed identities.

These investigative methods must be strictly managed as they can be intrusive, give members access to sensitive information and have the potential to put police members and the public at risk. As a result, many of these methods are legislated and all are governed by specific processes to ensure these methods are:

- used in appropriate circumstances
- used lawfully and in accordance with the properly issued authority
- undertaken by properly trained employees or authorised persons acting on behalf of Victoria Police
- recorded and reported where required.

### Application

Policy Rules are mandatory and provide the minimum standards that employees must apply. Non-compliance with or a departure from a Policy Rule may be subject to management or disciplinary action. Employees must use the **Professional and ethical standards** to inform the decisions they make to support compliance with Policy Rules.

These Policy Rules apply to:

- Investigators
- Specialist support staff

# Rules and Responsibilities

## 1. Covert physical surveillance

- Covert physical surveillance may be required to support a range of activities, including the covert observation of places, people or things to gather intelligence or evidence of criminal activity. These Policy Rules do not apply to the following:
  - urgent short-term surveillance in response to an imminent crime where it is not possible to obtain the services of an approved surveillance unit
  - short-term surveillance for the purposes of effecting an arrest.

- Except when undertaking static physical surveillance, physical surveillance must only be performed by employees who have completed the approved training course. See **VPMG Investigations support** for the:
  - explanation of the three types of physical surveillance; static, foot and mobile
  - approved course providers
  - minimum qualifications required to perform specific types of surveillance.

- Members conducting physical surveillance must do so in accordance with the training provided and the standards set by the Surveillance Standards Council (see **VPMG Investigations support** for the role of the Council).

## 2. Undercover investigations

### *2.1 Overview*

- Undercover investigations are managed by the Undercover Unit, Intelligence and Covert Support Command (ICSC).

- An undercover investigation is defined as a police officer, including an officer or officers from other jurisdictions, acting in a covert capacity and tasked with communicating with a suspect or suspects for the purpose of obtaining evidence or intelligence.

- When an undercover investigation is required submit an Application for Covert Support [Form 923] to the Work Unit Manager, Undercover Unit in accordance with **VPMG Investigation support**.

- Undercover investigations do not include covert investigations that are managed by Professional Standards Command (PSC) and approved by the Assistant Commissioner, PSC.

- If the undercover investigation involves conduct that a person would be criminally responsible for, it must be managed as a controlled operation; see section 6 below.

- Undercover investigations are designated either Level one or two.

### 2.2 *Level one undercover investigation*

- Level one undercover investigations must:
  - only involve low level intelligence gathering or investigating minor offences such as licensing, gaming, vice or property but does not include online investigations
  - only involve low level interaction between the police member and the suspect
  - be actively supervised by a trained undercover controller
  - be approved by the Manager, Undercover Unit.

- Level one undercover investigations must not:
  - anticipate a police officer encountering violence or serious threats of violence
  - require a police officer to be in a covert role for an extended period of time
  - plan to use a human source to introduce a police officer to a target
  - deploy in circumstances where the risk cannot be adequately mitigated.

- Online investigations are not subject to this process, however the Undercover Unit's advice may be sought prior to such an investigation. The advice of the Undercover Unit must be sought in cases where an online investigation is likely to cross from the virtual to the real world.

- Police officers being deployed in a level one undercover investigation must:
  - ensure they are fully conversant with the operation order
  - have been fully briefed by a trained undercover controller
  - be physically and emotionally fit to undertake the deployment.

- Level one undercover investigations must be:
  - submitted on a Form 923
  - supported by Local Area Commander
  - forwarded to the Manager, Undercover Unit via Interpose for consideration and approval. The Manager, Undercover Unit will provide a link to the Interpose shell for this. See **VPMG Investigation support** for further
  - supported by an appropriate plan and risk assessment.

### 2.3 Level two undercover investigations

- Level two undercover investigations are all other undercover investigations not categorised as level one.

- Level two undercover investigations must
  - only be undertaken by trained operatives and controllers
  - only be conducted by the Undercover Unit
  - be approved by the Manager, Covert Services Division (CSD)
  - include an appropriate plan and risk assessment.

- Approval for level two undercover investigation:
  - before submitting a Form 923, obtain advice from the Operations Senior Sergeant, Undercover Unit.
  - submit Form 923 with a comprehensive target profile to the undercover unit. See **VPMG Investigation support** for further
  - the Form 923 must outline both the detail of the offence involved and the intelligence implicating the target
  - on recommendation from the Manager, Undercover Unit, applications for deployment are then considered by the Manager CSD, ICSC
  - the Manager CSD may reject or set any operational limitations , support requirements or any other relevant provisions
  - the relevant Interpose document record will record the approval or non approval, as well as the reason for the decision
  - approved applications will be returned to the Manager, Undercover Unit for implementation

## 3. Surveillance devices

### 3.1 Legislative authority

The *Surveillance Device Act 1999* makes provision for police members to install, use or maintain a surveillance device with any of the following:

- the express or implied consent of the parties involved
- a warrant or corresponding warrant
- an emergency authorisation or corresponding emergency authorisation
- to record a non-private activity.

### 3.2 Governance and Compliance

The Assistant Commissioner, ICSC is responsible for governance and compliance regarding surveillance devices.

### 3.3 Warrant applications

- An application for a warrant to use or retrieve a surveillance device must be made via the Special Projects Unit (SPU), ICSC, to the relevant issuing authority.

- Comply with the application procedure detailed in **VPMG Surveillance devices** when making this application.

- Investigators (other than PSC investigators) must not utilise the services of PSC or an external agency to make application for a warrant, without written authorisation from the Manager, Covert Services Division.

### 3.4 Joint Operations

In circumstances where a joint operation between Victoria Police and an external agency is being conducted, the following instructions must be complied with:

- the agency obtaining the surveillance device warrant (the primary agency) is responsible for all decisions regarding the execution of the warrant, and for the management of surveillance device/s used under the authority of the warrant; with the officer named in the warrant being the officer having primary responsibility

- the primary agency is responsible for all records and documents required to be kept in relation to the warrant and for reports required under the *Surveillance Devices Act*, notwithstanding the partnering agency may play a substantial part in creating and keeping the records

- the partnering agency can only act in relation to the warrant and devices used under the authority of the warrant with the agreement of the primary agency, or under documented guidelines approved by the primary agency

- the officer having primary responsibility for the warrant must be kept fully briefed by the partnering agency and must ensure the required records are kept, and that information obtained by the device/s used under the warrant is kept secure

- information obtained by a surveillance device used under the authority of a warrant belongs to the primary agency, not to the partnering agency, even where the partnering agency may have installed and monitored the device and recorded information

- the partnering agency must not use information obtained from a surveillance device under the authority of a warrant for any purpose other than the purpose of the joint investigation, unless the information is first formally communicated to the partnering agency, by the primary agency, for a permitted purpose (s.30F, *Surveillance Devices Act*)

- the primary agency is responsible for making all records and documents available for inspection by the Victorian Inspectorate (s.30P, *Surveillance Devices Act*).

- at the conclusion of the joint operation, the partnering agency must return all documents and information to the primary agency for appropriate retention and destruction under the *Surveillance Devices Act*, or the relevant records act.

Refer to section 5, **VPMP Crime reporting and investigations** for further information on joint investigations with government and law enforcement agencies.

### 3.5 Emergency authorisations

- Where it is not practicable to apply to a court for a warrant, an emergency authorisation may be issued by a senior officer in accordance with s.26(1) or s.27(1), S*urveillance Devices Act,* where there is:
  - an imminent threat of serious violence to a person
  - an imminent threat of substantial damage to property
  - a serious drug offence is being, has been, is about to be, or is likely to be committed.

- Refer to **VPMG Surveillance devices** for the definition of a senior officer and the procedure for making this application.

### 3.6 Placing a surveillance device

- The Technical Surveillance Unit (TSU), ICSC, is responsible for determining the placement of surveillance devices. In prescribed circumstances, the TSU may authorise a qualified Regional Covert Camera Installer (RCCI) to install and manage devices (covert cameras) on their behalf in accordance with **VPMG Surveillance devices**.

- Local work units must not deploy surveillance devices by any other means.

- In relation to PSC investigations, the PSC Technical Unit is responsible for placing the surveillance device.

### 3.7 Monitoring, reviewing and retrieving a surveillance device

- The member in charge of the investigation is responsible for monitoring the device and any information received as a result of the device. Where the continuous monitoring of a device cannot be ensured, a warrant for a device should not be sought.

- When the surveillance device is no longer required or the warrant is nearing expiry and its use is still required, refer to **VPMG Surveillance devices** for information on both extracting the device and extending the warrant's authority.

### *3.8 Protected information*

- Employees must treat all information, records, and reports obtained from the use of surveillance devices as protected. Protected information is defined in s.30D, *Surveillance Devices Act.* See **VPMG Surveillance devices** for details on permitted uses of protected information as provided by s.30E(4), *Surveillance Devices Act*.

- The investigating member is responsible for maintaining a Protected Information Register, which is obtained from SPU. Refer to **VPMG Surveillance devices.**

### *3.9 Investigating member's responsibilities*

- Recording and providing information as directed by the SPU.

- Maintaining a Protected Information Register obtained from the SPU.

- Storing the register and protected information material in accordance with the *Surveillance Devices Act 1999* and **VPMG Surveillance Devices**.

### *3.10 Reporting and inspection requirements*

- The law enforcement officer to whom a warrant has been issued (generally the Manager, Affidavit Preparation Section, SPU) must ensure a report regarding the use of the surveillance device is submitted to the issuing court within the specified timeframe. The investigating member is responsible for submitting a completed 'Particulars Required for Court' Report to the Evidence Preparation Section, SPU to facilitate this. Refer to s.30K, *Surveillance Devices Act*.

- The Chief Commissioner must submit an annual report to the Minister regarding Victoria Police use of warrants and emergency authorisations. The Work Unit Manager, SPU is responsible for the preparation of this report (s.30L, *Surveillance Devices Act*).

- The Protected Information Register must be inspected by the Manager of the Work Unit holding the register, as part of the regular workplace inspection process.

- Where accountable records or material are found to be missing, a report covering the full circumstances of the loss and detailing all efforts made to locate the missing records or material, must be made by the Manager of the work unit where the records or materials were last located. This report must be forwarded to the Assistant Commissioner of the relevant Region/Command in the first instance, with a copy forwarded to the Manager, SPU. The Assistant Commissioner of the relevant Region/Command must then inform the Assistant Commissioner, ICSC.

### *3.11 Storage and destruction of records*

- Under s.30H, *Surveillance Devices Act*, all records and reports associated with the use of a surveillance device must be:
  - stored in a secure place that is not accessible to people who are not entitled to deal with them
  - stored at a minimum, in a dedicated locked metal filing cabinet (material for separate investigations can be stored in the same cabinet if the drawers can be individually locked)
  - post committal stage, transferred to the regional/command central storage point as determined by the relevant region or command. Refer **VPMG Surveillance devices** for information on storage of surveillance device material post-committal stage
- When no longer required for a permitted purpose, all records and reports covered by the *Surveillance Devices Act* must be destroyed in accordance with **VPMG Surveillance Devices**. The Protected Information Register must not be destroyed without appropriate approval, in accordance with **VPMP Information review, retention and disposal.**

## 4. Telecommunication intercepts

The use of telecommunications intercepts and associated information is governed by the *Telecommunication (Interception and Access) Act 1979* (Cwlth) and *Telecommunications (Interception) (State Provisions) Act 1988*. See **VPM Telecommunications interceptions**.

## 5. Counter Terrorism Warrants

In accordance with **VPMG Counter terrorism**, any application for either a Preventative Detention Order or Covert Search Warrant pursuant to the *Terrorism (Community Protection) Act 2003* should be forwarded to SPU for finalisation of the affidavit and application to the Supreme Court.

# 6. Controlled operations

## 6.1 Legislative authority

The *Crimes (Controlled Operations) Act 2004* regulates the use of controlled operations by Victoria Police. A controlled operation consists of an operation, involving conduct for which a person would otherwise be criminally responsible, to obtain evidence that may lead to a prosecution of a person (s.6). See the legislation and **VPMG Controlled operations** for applicable definitions.

## 6.2 Application process

- To obtain authority to conduct a controlled operation, an application must be submitted on Interpose to the Controlled Operation Registry (COR). Comply with the application process in **VPMG Controlled operations** and section 4, **VPMG Drug Investigations**

- Where approval to conduct a controlled operation is urgently required outside of business hours, an application can be made by contacting the Duty Crime Officer (DCO). See **VPMG Controlled operations** for procedures. Urgent applications must be authorised by the Assistant Commissioner (Crime), these operations are considered to be high risk and will only be considered in exceptional circumstances.

## 6.3 Approval to conduct a controlled operation

- Applications for controlled operations must be assessed by the COR and progressed for consideration to the Serious Crime and Organised Crime Tasking and Coordination Committee (SCaOCTCC) before authorisation is obtained from the relevant delegate (see Misc. Delegation 2.8), or Authorising Officer, as follows:
  - cross border and local major controlled operations – a Deputy Commissioner or an Assistant Commissioner
  - local minor controlled operations – a Superintendent of the SCaOCTCC.

- The Authorising Officer must determine whether the application meets the relevant conditions within the *Crimes (Controlled Operations) Act*, taking into account:
  - the relevant matters provided in s.14-17, *Crimes (Controlled Operations) Act*
  - any additional matters specifically relating to the controlled operation; see **VPMG Controlled operations** and **VPMG Drug investigations**.

- The Authorising Officer must only authorise the application if all of the relevant legislative conditions within the Act have been met.

- Controlled operations must only be conducted for the duration which the authority is valid (s.19, *Crimes (Controlled Operations) Act*); see **VPMG Controlled operations** for applicable timeframes.

### *6.4 Varying and cancelling an authority*

Controlled operations must only operate in accordance with the authority that has been granted. Where it is necessary to vary or cancel the authority, the member in charge of the operation must seek approval from the Authorising Officer, as detailed in **VPMG Controlled operations** and **VPMG Drug investigations**

### *6.5 Conduct of the controlled operation*

- The Principal Law Enforcement Officer (PLEO) (see **VPMG Controlled operations** for definition) must ensure all participants are fully briefed on the operation to ensure it is conducted in accordance with the authority and within the limits outlined in the Act.

- Have regard to the **VPMG Controlled operations** and **VPMG Drug investigations** when managing the conduct of the operation to ensure that legislative requirements are met.

### *6.6 Handling of authorities and document security*

- Documents must be classified in accordance with **VPMP Information categorisation, collection and recording**.

- Only the COR are permitted to print and store the authority.

- The Controlled Operation authority must not be included in any brief of evidence, including a hand up brief. Have regard to the **VPMG Controlled operations** if the documents are subpoenaed.

- COR will answer subpoena requests ands assist with issues of public interest immunity.

### *6.7 Reporting requirements*

- Within two months of the expiration of a controlled operation, the PLEO must complete a Principal Law Enforcement Officer's Report (s.37); refer **VPMG Controlled operations.**

- The PLEO must submit a report to the COR as soon as practicable if, in the course of or as a direct result of an approved operation, the following occurs (s.34):
  - loss or serious damage to property
  - personal injury, see s.34, *Crimes (Controlled Operations) Act*; and **VPMG Controlled operations** for information on this reporting process.

- The COR is responsible for preparing reports on behalf of the Chief Commissioner for submission to the Victorian Inspectorate as required by s.38, Crimes (Controlled Operations) Act.

# 7. Assumed Identities

- As provided by the *Crimes (Assumed Identities) Act 2004*, authority to acquire and use evidence of an assumed identity must be given by the appropriate delegate from a specialist department (see Miscellaneous Delegation 2.10).

- Comply with the application process detailed in **VPMG Assumed identities** when seeking an authority to obtain evidence of an assumed identity.

- The person authorised to use an assumed identity must do so in accordance with the authority.

- Delegates are responsible for ensuring that records are kept as required by s.32, *Crimes (Assumed Identities) Act 2004* and retained/destroyed in accordance with **VPMP Information review, retention and disposal**.

- Records kept for the purpose of Part 6 of the *Crimes (Assumed Identities) Act* must be audited in accordance with s.33 Crimes (Assumed Identities) Act, Miscellaneous Delegation 2.15 details the specific positions within the specialist units that are appointed to conduct these audits; see **VPMG Assumed identities.**

# 8. External oversight

## *8.1 Victorian Inspectorate*

- The role of the Victorian Inspectorate is to inspect records to ensure compliance as detailed in s.30P, *Surveillance Devices Act,* s.18, *Telecommunications (Interception)(State Provisions) Act* and the *Crimes (Controlled Operations) Act 2004*.

- Employees must give all reasonable assistance to the Victorian Inspectorate and Victorian Inspectorate Inspection Officers to facilitate inspections.

- Except in the course of a Victorian Inspectorate inspection process, all communications with the Victorian Inspectorate and Victorian Inspectorate Inspection Officers must be made through the relevant Assistant Commissioner.

### *8.2 Public Interest Monitor*

- The Public Interest Monitor (PIM) is established through the *Public Interest Monitor Act 2011.* The PIM has powers in relation to the:
  - *Major Crime (Investigative Powers) Act 2004*
  - *Surveillance Devices Act 1999*
  - *Telecommunications (Interception) (State Provisions) Act 1988*
  - *Terrorism (Community Protection) Act 2003*
- The PIM has various functions including appearing at any hearing of an application relating to the above Acts to test the content and sufficiency of the information relied on and the circumstances of the application.
- The Affidavit Preparation Section, SPU must to provide a copy of any affidavit in support of a warrant pursuant to the above Acts to the PIM prior to the court hearing.
- Investigators must supply the Affidavit Preparation Section, with sufficient information to be included in the affidavit including any information, facts and matters that may be adverse to issuing the warrant. It is an offence for a member to knowingly or recklessly fail to fully disclose all matters of which the member is aware that are adverse to issuing the warrant.

## Quick Links

- VPMG Investigation support
- VPMG Surveillance devices
- VPM Telecommunications interceptions
- VPM Controlled operations
- VPMG Assumed identities

## Further Advice and Information

For further advice and assistance regarding these Policy Rules, contact the relevant work unit within Intelligence and Covert Support Command (e.g. State Surveillance Unit, Undercover Unit, Special Projects Unit) or the Controlled Operations Registry, Crime Command.

# Update history

| Date of first issue | 22/02/10 | |
|---|---|---|
| **Date updated** | **Summary of change** | **Force File number** |
| 24/09/12 | Inclusion of joint operations and further information on reporting, inspections, storage and destruction of Telephone Interception and Surveillance Devices records and Special Investigations Monitor. | 068905/11 |
| 07/01/13 | Amendments throughout the document to reflect changes to Crime Command investigation practices. | 072989/12 |
| 11/06/13 | New section 6 – process for s.287 Telecommunications Act 1997 information requests via PC D24 | 067539/11 |
| 18/11/13 | References to redundant instruments following IMSSD review have been updated with corresponding new instruments. | 069562/11 |
| 20/01/14 | Section 2 – Undercover investigations reviewed to reflect Undercover Unit approval processes | FF 074660 |
| 01/09/14 | Updated name of Technical Support Unit to Technical Surveillance Unit. | FF-078741 |
| 31/08/15 | Reference to new protocols for surveillance devices to be fitted and monitored by Regional Covert Camera Installers operating from local work units | FF-094996 |
| 16/12/19 | Removal of most of telecommunication interceptions section to avoid conflict with new policy **VPM Telecommunications interceptions** | FF-120951 |