Special Investigative Techniques:
A field guide for frontline officers

UNODC would like to recognize the contribution of the Government of Australia, the Government of Canada and the Government of the United States of America.

To view this publication from a mobile device or to access other UNODC publications, please scan the QR code.

This content is updated regularly with new information. For the latest version of content and to access other materials and tools please visit the QR code.

Special Investigative Techniques:

A field guide for frontline officers

This publication contributes to Sustainable Development Goal 16 that seeks to: "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels"

The Sustainable Development Goals are the blueprint to achieve a better and more sustainable future for all. They address the global challenges we face, including those related to poverty, inequality, climate, environmental degradation, prosperity, and peace and justice. The Goals interconnect and in order to leave no one behind, it ís important that we achieve each Goal and target by 2030.

INTRODUCTION

The investigation of transnational organised crime requires law enforcement agencies to adopt and utilise advanced investigation techniques to collect intelligence and evidence that can be used to dismantle criminal networks and thus have the greatest impact on organised crime.

Many of these special investigative techniques require specialist training and equipment and should not be undertaken unless you have received this training. In addition, the use of many of these techniques require authorisation by a Court or Senior Officer and should only be used if you have received the necessary authority to do so.

You should carry this field guide with you while you are on duty. It contains quick-reference tools to address situations you are likely to experience in the course of your duty.

Table of Contents

1. SPECIAL INVESTIGATIVE TECHNIQUES

Special investigative techniques are those techniques used by law enforcement agencies that require specialist training and/or equipment and are generally covert in nature.

Examples of advanced investigative techniques and ones that will be addressed in this handbook include:

- Undercover investigations
- Surveillance
  - Physical
  - Electronic
- Controlled Delivery
- Telecommunications Interception

These techniques are frequently used by law enforcement agencies and can be invaluable tools to gather evidence against members of organised crime groups and can assist in the detection and prevention of crime.

However, there risks associated with the use of these techniques including potential compromise of the investigation and danger to the police involved. Accordingly, these techniques are best employed by law enforcement officers who have received the necessary training in their use and application.

These techniques may also require permission from a senior officer or court before they can be employed so you should check the policies, procedures and regulations in your jurisdiction.

One area that is not technically a special investigative technique but one that will also be included in this manual because of its potential value on the investigation of organised crime is Informant Management.

Adopted by General Assembly resolution 55/25 of 15 November 2000, the United Nations Convention Against Transnational Organised Crime (UNTOC) is the main international instrument against transnational organised crime. Signed in the Italian City of Palermo in December 2000 the Convention entered into force on 29 September 2003. All members states of the Greater Mekong Sub-region are signatories to the UNTOC Convention.

The UNTOC contains 41 articles, several of which are important for law enforcement agencies investigating transnational organised crime.

Article 2 of the Convention contains definitions that may be important for the use of advanced investigative techniques and these include;

a. "Organised Criminal Group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;

b. "Serious Crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;

c. "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

d. "Predicate Offence" shall mean any offence as a result of which the proceeds have been generated that may be subject to money laundering provisions contained within UNTOC

2. UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANISED CRIME

e. "Controlled delivery" shall mean the technique allowing illicit or suspect consignments to pass out of, through or into the territory of one or more States, with the knowledge and under the supervision of the competent authorities, with a view to the investigation of an offence and the identification of persons involved in the commission of the offence.

The UNTOC also has provisions for Mutual Legal Assistance (Article 18), for Joint Investigations (Article 19) and Special Investigative Techniques (Article 20).

Special Investigative Techniques includes electronic and other forms of surveillance, undercover operations and controlled deliveries. These methods will be examined in this handbook.

You can find the UNTOC at this link https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html#Fulltext

3. NATIONAL LEGISLATION

Generally, it is permitted to use the full range of special investigative techniques including controlled delivery, for investigations into drug and terrorism related crimes.

However, in some countries within the region the legal framework is not clear as to whether these techniques can be used in relation to other crime types, such as wildlife and human trafficking.

You should make yourself aware of the relevant pieces of legislation within your country that address special investigative techniques and determine if and when you can utilise these methods. If you are in doubt consult with a Senior Officer from your department or from the Prosecutor's Office.

4. UNDERCOVER INVESTIGATIONS

Undercover investigations by their very nature require a police officer, or informant legally acting under the direction and authority of a police officer, to engage and deceive a criminal suspect with the view to collecting intelligence or evidence of a crime.

Undercover operations may be classified as

- Impromptu.
- Short.
- Long.
- Penetration.

Objective of an undercover investigation

- Obtain intelligence or evidence not available through other investigative techniques.
- Observe the criminals planning a crime.
- Observe the crime.
- Purchase contraband.
- Collect evidence of past crimes.
- Identify members of a criminal network.
- Corroborate intelligence or information received from informants.

Five Phases of an undercover investigation

- **Planning**
  - Collection information and intelligence on the suspect.
  - Research the alleged crimes.
  - Is an undercover operation the most appropriate response?
  - Identify entry point for undercover operative.
  - Well planned role and documented legend of the undercover operative (UCO).
  - Risk planning to ensure safety of the UCO.

- **Initiation**
  - What is the most appropriate course of action to engage the suspect?
- Use of an informer.
- Chance encounter.
- Cold call.
- Lure the suspect.
- Operational
  - Is geared towards achieving objectives.
  - Is sufficiently resourced and staffed.
  - UCO security is paramount.
  - Is following timeframes established in planning phase.
  - Is conducted ethically.
  - Chain of custody.

- **Termination**
  - Undercover Operations are terminated when:
- Goals have been achieved.
- Goals have not been achieved.
- Operation has been compromised.
- **Evaluation**
  - Evaluation of the undercover operation to identify if it has met its objectives.
  - Investigation was conducted ethically and within legal frameworks.
  - Chain of custody for evidence has been maintained.
  - UCO performance.
  - What lessons were learnt.

Not all police are suited to perform in an undercover capacity and those who do should receive specialised training. Traits of a good UCO include;

4. UNDERCOVER INVESTIGATIONS

- Self confidence
- Calm under pressure.
- Likeable personality.
- Adaptability and ingenuity.
- Ability to analyse situations and make sound decisions.
- Good observation skills.
- Appropriate physical appearance.
- Understanding of the subject matter.
- Ethical.

Legend

UCO's are required to create a persona for themselves and to 'become' that person when performing in an undercover role. To do this successfully it is best that you base your UCO legend as close to your real personality as possible. You should also support your legend with official documentation in your UCO name. Remember that when you are performing in an undercover capacity you should have nothing on you, including telephones, wallets, clothing or documentation that may indicate that you are a law enforcement officer.

Gaining Confidence of a Suspect

The role of a UCO is to gain the trust of a suspect so that they engage in criminality in the presence of the UCO or they discuss their involvement in crime. There are several things that a UCO can do to gain the confidence of the suspect, including:

- Know your products.
- Know your prices.
- Know the market.
- Be prepared to bargain.
- Be prepared to walk away.

- Show the same degree of caution as the suspect.
  - Fear of being robbed.
  - Fear of being arrested.
  - Have answers prepared for the hard questions when they come from the suspect, such as;
  - You are a police officer?
  - Who do you know in the business?
  - Who can vouch for you?
  - How did you get my number?

Role of the Investigator

- Identify your objectives and constantly assess the progress of the investigation
- Brief and debrief the UCO.
- Listen to the recordings and view any messages between the UCO and suspects
- Ensure the welfare of the UCO.
- Update your supervisors.
- Ensure chain of custody of any evidence collected during the investigation
- Prepare the case file.
- Ensure sufficient resources are available to cover meetings between the UCO and suspects.

At all stages of an undercover operation the safety of the UCO is paramount. If it is too dangerous, don't do it. You should only use officers who are trained in undercover investigations to perform in an undercover role.

Always abide by the rules of your jurisdiction in relation to the use of undercover operatives.

4. UNDERCOVER INVESTIGATIONS

Online Undercover Investigations

Online investigations are a valuable tool for law enforcement agencies to collect evidence and intelligence in respect to many crime types, but in particular paedophilia, human trafficking and wildlife trafficking.

Many of the same principles will apply with online undercover investigations as physical investigations. However, should you communicate with suspects online with a view to collecting evidence remember to:

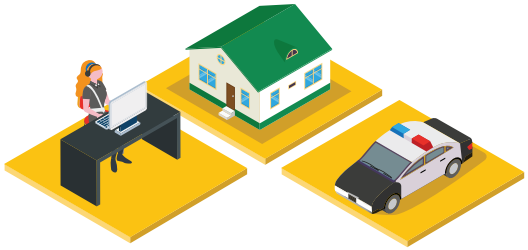
- Ensure that your actions are legal within your jurisdiction
- Ensure that you have sought the permission from your supervisor
- Always use a covert account
- Screenshot the suspects profile – this can be changed by them at a later date
- Screenshot any messages between you and the suspects
- Record any videos or messages they send to you
- If possible do not share your photograph with a suspect
- If possible do not post your photograph on your covert profile
- Refrain from talking via video with the suspect
- Ensure chain of custody of any evidence you collect.

Surveillance is the covert monitoring of persons, places or things, in order to obtain information or evidence.

Surveillance is a valuable law enforcement tool that is effective at detecting, preventing and collecting evidence of criminal activity. Surveillance can be broken down into two areas, physical surveillance and electronic surveillance, although many investigations will combine both types.

Objectives of surveillance

- Obtain evidence of a crime.
- Identify suspects or criminal connections.
- Gather intelligence.
- Lifestyle assessment.
- Support undercover deployments.
- Asset protection.



Basic physical surveillance principles

Some basic surveillance principles that can be applied to any form of surveillance include;

- Eyeball
  - The eyeball is the person who can see the suspect and has priority in communications.
- Back up
  - Supporting other surveillance operatives.
- Handovers
  - Changing the eyeball.
- Rotation
  - Moving team members around to minimise exposure.

5. PHYSICAL SURVEILLANCE

- Communication
- The eyeball speaks or gives permission to speak.
- Dress Up to Dress Down
  - Wear clothing that does not stand out but allows you flexibility to go to different types of locations.
  - Props that support your reason to be there.
- Elastic Principle
  - In heavy traffic get closer to suspect - particularly in cities.
  - In light traffic – give yourself space - particularly in rural areas.
- Stopping
  - When the suspect stops, describe location.
  - Establish your safety net – place operatives in locations to cover potential movements
  - Control the natural exit – where suspect is most likely to go.
  - Research and cover other exits
- Plotting
  - Place your surveillance team in a location to 'box' in the suspect.
  - Eyeball on suspect.
  - Extend your team along natural exit with a view to other potential exits.
- Total Loss of suspect
  - Declare early.
  - Define and describe point of loss.
  - Any intelligence on where suspect may be heading.

Briefings

Prior to the deployment of a surveillance team you should thoroughly brief them on their objectives and provide them as much detail on the target(s) as possible. Your briefing should include`;

- Target profile
- Target name/pseudonym
- Target photo
- Associates
- Places frequented
- Officer safety issues
- Vehicles
- Communications protocols

Communications

Good communication skills and protocols are essential for effective surveillance. If possible, specialised encrypted radios should be used. If these are unavailable there are many encrypted mobile applications can be utilised that provide some degree of security and flexibility. These applications are also time stamped, enable quick location exchanges through dropping pins, allow for the sharing of text, talk, photographs and video and group chats. Examples include:

- WhatsApp
- Viber
- Line
- Skype
- Zoom

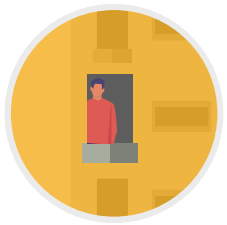
Surveillance logs

It is important that a contemporaneous log is maintained during surveillance. This log is a record of the activities observed during the surveillance including the who, why, why, when and how of the surveillance activities.

- A new log commenced for each day
- Chronological order
- Photos and videos identified
- Each entry initialled by surveillance operatives responsible
- All officers sign log

Types of physical surveillance:

- Static
- Foot surveillance
- Mobile surveillance – vehicle/motorcycle
- Aerial
- Marine



Static surveillance – Observations Posts

Static surveillance offers investigators the opportunity to view locations for a long period of time. The selection of an observation post is crucial as safe entry and exit is essential for the security of the officers involved and to reduce the risk of compromise. Factors that you should take into account when identifying an observation post include:

- Good view of target area
- Environment – hostile factors
- Access
- Weather conditions
- Toilet facilities
- Equipment
- Manned or remote monitoring

Foot surveillance

Foot surveillance is performed when your suspect is on is on foot or on public transport. Foot surveillance enables surveillance officers to get in close to suspects to observe and/or record conversations, exchanges and other behaviour.

Foot surveillance requires flexibility and patience on behalf of the surveillance operatives. Important things to remember during foot surveillance include:

- Clearing corners
  - When the suspect nears a corner, teamwork is needed to ensure they don't double back on the surveillance operative.
- Hand signals
  - To signal if the suspect has stopped or continued, particularly as they round comers.

- Marking
  - When suspect used ATM, public telephones, buys SIM cards etc.

Mobile surveillance

Mobile surveillance of suspects requires teamwork, coordination and good communication skills. Important factors for mobile surveillance include:

- Sufficient vehicles and surveillance operatives for combined mobile/foot surveillance
  - Be cautious of compromise when undertaking surveillance with less than six operatives – the more operatives the better.
- Vehicles used for surveillance should be a combination of different types including 4x4's and motorcycles.
- Consider the use of a taxi as a surveillance vehicle.
- Elastic principle.
- Utilise props in vehicles.
- Avoid using vehicles associated with police cars.
- A good 'lift off' (following suspect when they initially move) is important for effective surveillance
- Drive naturally
- If possible, utilise tracking devices to assist in the surveillance

Aerial/Marine surveillance

Aerial and marine surveillance require specialist equipment and trained staff. These can enhance and support physical surveillance teams but can be very expensive. Ensure that you have sought the permission of a senior officer before you deploy these assets.

Technical surveillance is the monitoring of behaviour, activity of locations by electronic means. It can include:

- Audio/video recording devices
- Tracking devices
- Telephone interception

Audio/Video recording devices:
The recording of a suspect making admissions in relation to a crime is powerful evidence. Similarly, suspects recorded planning a violent crime enable law enforcement officers to prevent or deter those suspects.

The reduction in the size and quality of video cameras has also revolutionised covert surveillance. Gone are the grainy black and white images, now to be replaced with high definition colour footage with.

Given that the covert recording of people in their homes/offices, on their telephones or in their vehicles is an invasion of their privacy these techniques should only be used proportionally and with legal approval.

Audio/video recording devices come in a variety of sizes and shapes. Typical off the shelf products containing integrated Wi-Fi capable audio and video devices are readily available. Several of these devices are battery operated so this needs to be taken into consideration when you deploy them. Examples of these devices include:

- Power boards.
- Charge stations.
- Clocks.
- Body cameras.
- Lamps.
- Phone battery packs.
- Watches.
- Smoke detectors.

6. TECHNICAL SURVEILLANCE

Audio and video devices may also be hard wired and installed in premises and vehicles. The placement of these devices is important not only in relation to the value of the evidence you may collect but also for privacy reasons. You will also need to identify a location where these devices can be monitored and how you will monitor and record the information obtained from them. Potential locations for listening devices in premises include:

- In ceilings.
- Inside lounge chairs.
- Behind light switches/power points
- Behind drywall
- Air conditioning vents.

Hard wiring of listening devices inside premises can risk contact with live electricity. Ensure that this is undertaken by qualified electricians (preferably working for the law enforcement agency) or specialist police.

Potential locations for listening devices in vehicles include:

- In headrest
- In air conditioning vents
- Behind dashboard

Tracking Devices

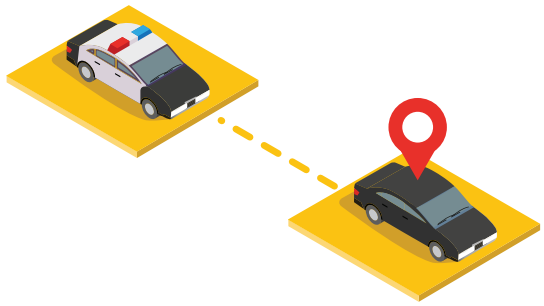
Tracking devices have also advanced in recent times and are now smaller but with a greater battery life. Older models of devices were either passive i.e. recorded information that could be analysed after retrieval, or active which recorded and transmitted data in real time. Generally tracking devices are now active but with improved functionality allows the reporting time to be varied and extending battery life.

GPS tracking devices generally report in one of three ways or a combination of these;

- Global Positioning System (GPS).
  - Use GPS to communicate with the tracking device.
- Global System for Mobile Communications (GSM).
  - Uses the telephone network to communicate with the tracking device.
- Ultra-High Frequency (UHF).
  - Requires a UHF device to pick up the tracking device, frequently used on animals

Tracking devices can be deployed in or on:

- Vehicles
- Vessels
- Aircraft
- People
- Containers
- Packages



Important things to consider when deploying GPS trackers:

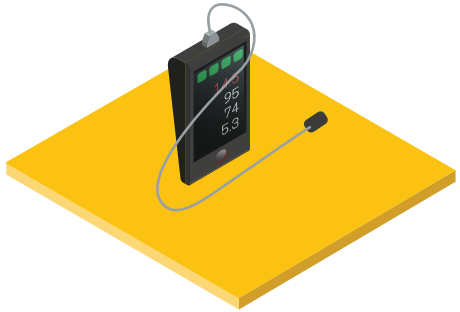
- Test tracker in or on under similar circumstances.
- If you need to covertly deploy it on a vehicle you should practice on vehicles of a similar make and model.

GSM tracking will also require access to a telephone network and a SIM card that needs to be charged. Some providers supply a global SIM card with credits that can be topped up. Take this into account when determining the device, you will use. If you suspect frequently attends locations outside of GSM coverage or in areas of poor coverage, consider using a GPS device. Many leading GPS brands provide trackers with both GPS and GSM capabilities.

The deployment of tracking devices can be dangerous, and police have been killed by suspects while deploying them. These devices should only be deployed by trained officers who have surveillance support.

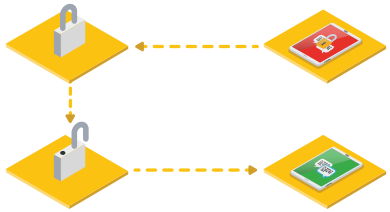
Telephone Interception:

The monitoring of telephone calls has been a standard tool used by law enforcement in the investigation of crime for many years. In some jurisdictions the intercepted telephone calls of suspects may be used as evidence while in others it can only be used for intelligence purposes. In most jurisdictions the interception of a telephone service requires an authority from a court.



In recent times the advent of web-based encrypted communication applications and the increased sophistication of smart phones have provided criminals with greater flexibility, anonymity and security to facilitate their crimes. Many criminals have moved to applications such as WhatsApp, WeChat, Viber, Line, Messenger and Wire to make and receive telephone calls and send and receive messages. The end to end

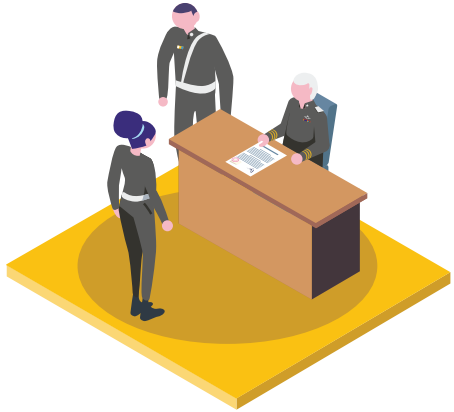
encryption services offered by these applications has made the job of law enforcement much harder as these systems are very difficult to intercept with current technology.



Despite the issues posed by encryption the interception of telephones can still be a useful investigative tool. In some instances, criminals do not use the more secure features on their telephones and speak freely on systems that can be intercepted. While even those that use the encrypted applications on their phones may still communicate with others on less secure systems.

One issue that will need to be addressed both before you intercept the suspects telephone and during interception is attributing the use of the telephone to the suspect. Phone attribution is crucial to prove that the voice on the telephone is the suspect. This can be done in several ways.

- Before interception
  - Billing details
  - Analysis of call records
  - Information received from an informant
  - Other government records



- During interception
  - Suspect states their name
  - Suspect calls family members or friends
  - Information stated during call corroborated by surveillance
  - Suspect orders and receives deliveries
  - Suspect pays for bills using telephone
  - Suspect makes or receives telephone calls to/from employer

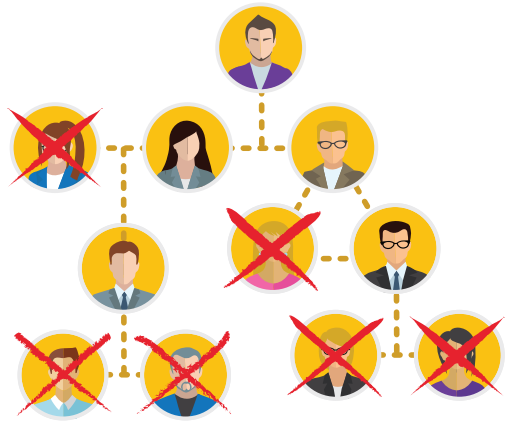
Before you intercept the telephone service of a suspect ensure that you have the legal authority to do so.

Criminal networks transport huge quantities of contraband around the globe every day utilising freight forwarding services or couriers. Often the documentation accompanying these shipments contain fictitious names, addresses and contact numbers which makes it difficult for law enforcement agencies to detect the true senders or recipients of the products. In addition to this problem even if law enforcement can identify the intended recipient it is often difficult to prove that they had knowledge of the contents of a container or package. To address this problem law enforcement agencies often utilise a controlled delivery.

A controlled delivery is a highly effective investigative technique involving the transportation of contraband to a suspect while it is under the direction or surveillance of law enforcement officers.

Controlled deliveries are used to;

- Identify, arrest and convict offenders who facilitate, manage and direct the smuggling of contraband on a national, regional or global scale.
- Disrupt and dismantle criminal organisations engaged in smuggling contraband.
- Broaden the scope of an investigation to identify additional and higher-level offenders and obtain further evidence of criminality.
- Establish evidentiary proof of a suspect's knowledge of a crime.



Types of controlled deliveries

- Cold convoy – no knowledge by suspects.
- Using a cooperating suspect or informant.
- Mail and/or courier delivery.
- Delivery by undercover officer.

Preparing for a Controlled Delivery

- Are controlled deliveries allowed in your jurisdiction?
- Controlled deliveries can be expensive operations and run the risk of losing some of the seized contraband, have you sought permission from a Senior Officer?
- Do the potential benefits outweigh the risks? Have you undertaken a risk assessment?
- Do you have sufficient resources to undertake to undertake the operation?
- Do you need to liaise with other law enforcement agencies?
- Can you substitute you the majority of the contraband?
- Do you have the time to do a controlled delivery?
- Does the suspect expect a specific person to deliver the contraband?

Contraband Substitution

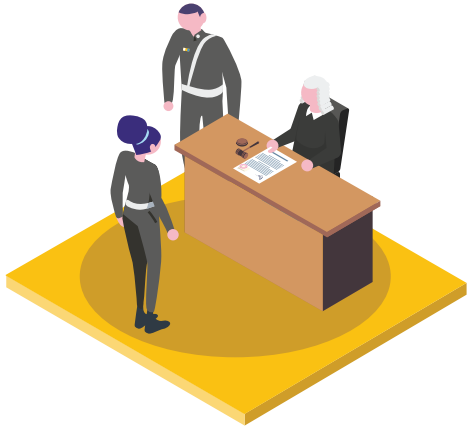
- Maintain (if possible) original packaging.
- If possible, remove the majority of the contraband.
- Replace with inert item(s) of a similar weight
- Record the substitution process and secure evidence.
- Check for possible physical evidence, fingerprints and DNA.

Undertaking a Controlled Delivery

- If possible, maintain original packaging.
- Insert tracking devices and recording equipment into the container/ packaging.

- Obtain you search warrant as soon as you identify the location where the package is to be transported but be prepared to amend the location if it is subsequently moved by the criminals.
- Maintain electronic and physical surveillance on the contraband.
- Deliver to the intended address or wait for the suspect to pick up the package.
- Monitor the listening device/covert camera to determine if the suspect has opened the package.
- If you don't have cover electronic surveillance, allow sufficient time for the suspect to inspect and open the package.
- Have your raid team on standby for when the suspect opens the container/package
- Once the suspect has opened the package and you have evidence of them inspecting it or discussing the contents execute the raid.
- Be flexible and patient in your approach, sometimes suspects may let a container sit unopened for weeks or longer to ensure that it is not under police surveillance.

Evidence of knowledge



- Recipient admits knowledge.
- Recipients opens package.
- Separates packages containing contraband.
- Admissions on covert recordings.
- Receiver attempts to flee upon opening of package or arrest.
- Forensic evidence.
- Access secret compartment.

An informant is a person who secretly provides information to law enforcement agencies.

Informants may have different motives for giving information, including for money, for revenge, to eliminate competition, to boost their ego or for goodwill.

When meeting an informant

- Make an official record of the meeting
- Meet in a safe, predetermined location
- Identify a safe route to and from the meeting place
- Develop a cover story for you and the informant in case you are seen meeting together
- Have another officer present during the meeting

8. MANAGING INFORMANTS

When communicating with an informant

- Develop nicknames for each other
- Use a new phone or SIM card that cannot be traced or used for any other purpose
- Develop rules and procedures for contacting each other
- Ensure the informant tells no one about assisting you
- Avoid meeting at offices, police stations, bars, etc.

Remember

- Abide by your agency's standard operating procedures on informant handling.
- Do not disclose the identity of the informant to anyone who does not need to know.
- Maintain a professional relationship with the informant. The informant is not your friend.
- The informant's safety is paramount, so develop contingency plans.
- Stay in control of the informant.
- Be available when the informant needs you.

9. EVIDENCE MANAGEMENT AND SECURITY

Evidence management

Evidence collected utilising special investigative techniques may need to be secured and access restricted to investigators who are authorised or named in a warrant/authority. Do not allow unauthorised access to the evidence. You should be familiar with the policies and procedures of your department around evidence storage and access.

Evidence collected by special investigative techniques will often be stored on electronic storage devices. You should never use the original devices to review the evidence collected or alter or change the original recording. You should always;

- Identify and label the original recording.
- Make working copies of the original.
- Store the original in a cool location with restricted access.

You also need to ensure chain of custody of any evidence you collect.

Evidence security

There may be restrictions on how evidence collected by special investigative techniques can be shared with other law enforcement agencies or when served upon a suspect or their legal representative.

Many of these restrictions are to protect the methods by which the evidence is collected and/or to maintain operational security.

You should be familiar with the policies and procedures of your department around disclosing of evidence or intelligence collected using special investigative techniques.

Regional Office for South East Asia and the Pacific
United Nations Building, 3rd Floor B Block, Secretariat Building
Raj Damnern Avenue, Bangkok 10200, Thailand
Tel. (66 - 2) 288 100 Fax (66 - 2) 281 2129 E-mail: fo.thailand@unodc.org
Website: www.unodc.org/southeastasiaandpacific