College of Policing

college.police.uk

Undercover policing

Authorised Professional Practice

For consultation: 29 June to 10 August 2016

Please send feedback to:

UCappfeedback@college.pnn.police.uk

Undercover policing

A number of covert tactics are available to law enforcement to prevent and detect crime or disorder and maintain public safety. Undercover is one of them.

Applied correctly and supported by appropriate training, undercover is a proportionate, lawful and ethical tactic which is effective in obtaining evidence and intelligence.

Contents

See also a statement from Chief Constable Jon Boutcher, National Policing Lead for Undercover.

1. Accreditation

The undercover accreditation process is designed to help forces and agencies deliver undercover operations safely, ethically and lawfully.

Main points:

- all units that deliver undercover operations should be accredited
- accreditation requires up-to-date self-assessments confirmed annually and validation visits at least every three years
- there is internal and external oversight and governance for undercover.

Contents

1.1 Accreditation process

All units that manage undercover operations should undertake a self-assessment process for accreditation to deploy undercover operatives.

This process is based on a three-year cycle, as follows:

1.1.1 All units complete a self-assessment

Self-assessment describes the undercover authorisation, governance and tactical management arrangements units have in place. The descriptions set out how units manage foundation and advanced undercover activity.

1.1.2 Units may be accredited based on their self-assessment

The category of accreditation determines whether units can manage foundation and/or advanced deployments.

1.1.3 Accredited units update and certify their self-assessments

Units should update their self-assessments when significant changes occur to their structure or operating practices and certify the accuracy of assessments annually.

1.1.4 Accredited units are visited by College of Policing validators at least every three years

Validators will make recommendations to the College of Policing accreditation registrar about whether the unit should continue to be accredited or whether the accreditation should be amended or withdrawn.

1.1.5 The College of Policing registrar reaccredits units based on the outcome of validation visits

The content of annual self-assessments, or failure to submit annual updates, may trigger a validation visit or cause accreditation to be withdrawn. If the accreditation registrar becomes aware of concerns about a unit's performance, they may arrange a validation visit or withdraw accreditation with immediate effect.

Units can also receive practice advice and support from the National Undercover Working Group.

1.2 Oversight and governance

The following provide oversight and governance to undercover:

- College of Policing
- Office of Surveillance Commissioners
- Investigatory Powers Tribunal
- Crown Prosecution Service
- Her Majesty's Inspectorate of Constabulary.

See also the authorising officer and senior responsible officer role descriptions in chapter 3.

2. Undercover operatives

Undercover operatives (UCOs) are members of a law enforcement agency who are selected, vetted, trained and accredited to gather intelligence and evidence.

Main points:

- UCOs are law enforcement personnel trained to carry out deployments
- there are two categories of UCO
- the foundation programme is the single point of entry for staff who want to become a UCO
- deployment and development options include progression to the advanced programme
- a UCO's eligibility to deploy can change over time
- undercover units operate a risk-based tenure policy.

Contents

2.1 Legislation

UCOs are deployed under direction in an authorised investigation or operation as a **covert human intelligence source** (CHIS).

Section 26(8) of the Regulation of Investigatory Powers Act 2000 (RIPA) defines a person as a CHIS if:

> (a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);
> (b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
> (c) he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

Statutory Instrument 2013/2788 further clarifies a UCO as a **relevant source** within a number of defined law enforcement agencies.

Relevant sources operate at a higher level of scrutiny and management than members of the public recruited as CHIS.

2.2 Features of the role

The role of UCO is voluntary, but all UCOs need to:

- comply with the UCO code of conduct
- maintain an up-to-date profile on the national undercover database
- create and maintain legends.

All UCOs have successfully completed nationally-licensed training. They maintain accreditation through continuing professional development (CPD).

The roles, responsibilities and conduct of individual UCOs should be commensurate with their skills, knowledge, ability, training and experience.

2.3 Categories of UCO

There are two categories of UCO:

- undercover **foundation** operatives (UCFs)
- undercover **advanced** operatives (UCAs).

Undercover **online** operatives (UCOLs) are either UCFs or UCAs.

2.3.1 Foundation operatives

UCFs carry out low-level infiltration that does **not** require the ability to withstand intense scrutiny. After initial training, UCFs can attain additional modules which enable them to be deployed on a greater range of duties. For example, online or street drug buyer.

UCFs undertake CPD to maintain their accreditation and so that they can be deployed in specialist subject areas. UCFs can be deployed with UCAs, but only in limited supporting roles.

2.3.2 Advanced operatives

UCAs are trained to undertake deployments involving higher-level infiltrations in a leading role with the ability to withstand intense scrutiny.

UCAs undertake CPD to maintain their accreditation and so that they can be deployed in specialist subject areas.

2.3.3 Online operatives

UCOLs are either foundation or advanced UCOs.

They are operatives who are deployed to establish and maintain relationships with an individual, network or organisation through the use of the internet with the covert purpose of obtaining intelligence, information or evidence as part of an authorised operation.

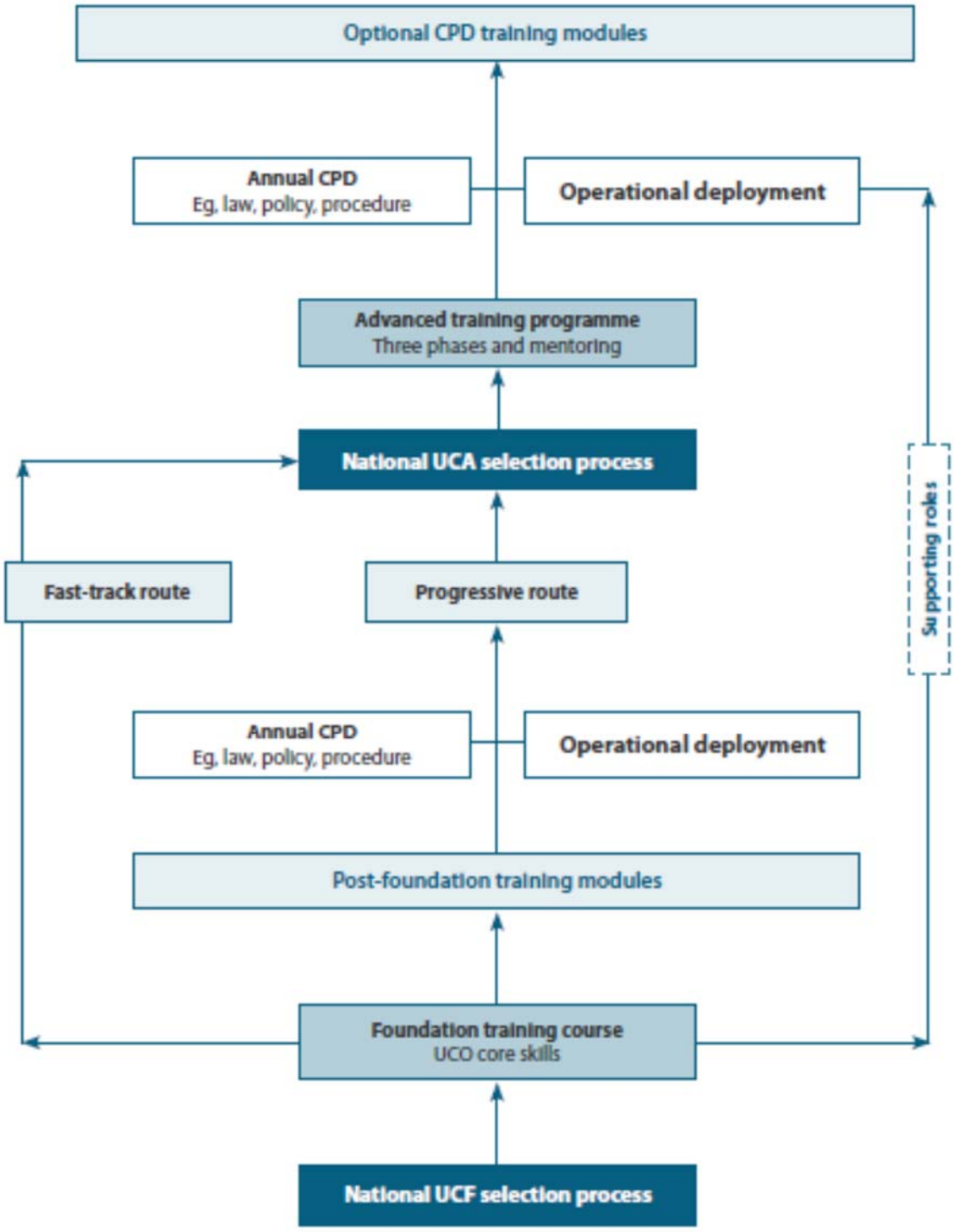
UCOLs include staff previously described as covert internet investigators who have been awarded ‘grandparent rights’ as a UCF to perform the role of UCOL. They are identified on a national index.

See also the section on online operations.

2.4 Selection, training and development

There is a standard selection, training and development process for staff who want to do UCO work.

This is a depiction of the overall structure – it reads from the bottom up.



The foundation programme is the single point of entry. The successful completion of additional training and assessment from foundation to the advanced programme determines the extent of the planned involvement of the UCO.

To operate as a UCOL, individuals should complete the approved online undercover course.

2.5 Eligibility to deploy

A UCO's status can change over time. In order to be deployable, a UCO must be deemed to be **active**.

Absence of any of the qualifying criteria in the active status category will result in the UCO being recorded as **dormant** on the national database or removed from it.

Such UCOs require an individual development plan before they can be deemed active. This development plan and their return to active status should be endorsed by the COM-UC (covert operations manager for undercover).

UCOs not supported by the COM-UC to remain on the national database will be removed.

2.5.1 Qualifying criteria

The qualifying criteria for active status differs for UCFs and UCAs:

Active status is achieved by satisfying the following	UCF	UCA
Deployed in the last 24 months	✓	✓
Undertaken CPD (local, role-specific and national) in the last 12 months	✓	✓
Signed the UCO code of conduct on an annual basis	✓	✓
Registered on the national database with an up-to-date profile	✓	✓
Subject to an approved legend	×	✓
In possession of valid backstopping	×	✓
Attended psychological assessment within the previous six months	×	✓
Supported by the respective COM-UC	✓	✓

2.6 Tenure

Undercover units should ensure UCOs reflect the skills and profiles of current and future criminality. This may require staff turnover, using full and part-time UCOs and retiring those who no longer reflect the skills or profile needed.

Undercover work can expose operatives to unusual stressors that are not common to everyday law enforcement activity. Long-term sustained undercover activity can lead to:

- identity issues
- affiliation with the groups or individuals being investigated
- difficulties in maintaining personal relationships
- degradation of general law enforcement skills and knowledge.

Tenure periods need to be balanced to achieve value for money on the investment made in a UCO against the stressors involved in undercover work. See also the chapter on welfare.

The level of psychological strain, the rate at which skills fade and changes in operational strategy differ. For this reason a fixed-term tenure cannot meet the needs of all undercover units. Instead UCOs are assessed by their COM-UC according to a risk-based tenure policy agreed by the National Undercover Working Group.

2.7 Foundation programme

The foundation selection process has been designed by the College of Policing to identify staff with the potential to be effective UCFs.

2.7.1 Selection process

There are seven stages to the UCF selection process:

1. advertising
2. regional open day
3. preview and questionnaire
4. application form and sifting
5. conduct and discipline checks

6. personality assessment
7. assessment through exercises.

Candidates who are recommended after completing this selection process secure a place on the UCF training course.

They must pass this course to become a UCF.

2.7.2 Core competencies

UCF skills are broadly defined by core competencies which underpin the selection process:

- social skills (social intelligence)
- communication skills
- commitment and drive (motivation)
- resilience and confidence
- self and team development
- professionalism (including integrity)
- undercover credibility
- creative planning
- dynamic decision making
- effective evidence and administration
- knowledge, research and preparation.

2.7.3 Legal input by distance learning

Candidates who pass the seven stages of the UCF selection process are given a distance learning pack. This pack covers legal input that the candidate needs to work through before starting the UCF training course. It gives details on the legislation, case law and procedures relevant to undercover policing.

2.7.4 Training course

The UCF training course focuses on the core skills and behaviours required to operate in a wide range of operations. The course is competency-based and students are assessed as competent or not.

Commodity-based skills (eg, purchasing drugs) do **not** feature in the initial course. They are delivered by additional training where required.

Individuals will **not** be deployed operationally until they have successfully completed the national foundation training course.

2.7.5 Post-foundation development

The post-foundation development received by a UCO determines the type of undercover operations or responsibilities they can undertake and the type of undercover tactics they can employ.

UCFs undertake CPD to maintain their accreditation and can progress to the advanced programme.

2.8 Advanced programme

The advanced selection process has been designed by the College of Policing to identify UCFs with the potential to be effective UCAs.

2.8.1 Pathways to selection and training

There are two pathways to selection and training for the UCA role:

1. **Progressive route** – UCFs who have undertaken continuing professional modules and who, through their operational UCF deployments, have demonstrated the skills and experience required to operate at an advanced level can be considered for UCA selection and training.
2. **Fast-track route**
    a. UCFs who demonstrate a high level of skill during foundation training but who have not yet been operationally deployed as a UCF may be considered for UCA selection and training.
    b. In exceptional cases, an individual may be identified who is not a UCF but who is believed to have the potential skills to be a UCA. In these circumstances the individual will be required to complete the foundation course before commencing the advanced programme.

The national UCA selection process applies to both pathways.

2.8.2 Selection process

The national UCA selection process is delivered at a national level and coordinated by the College of Policing.

There are six stages to the UCA selection process:

1. advertising
2. national open day
3. preview and questionnaire
4. application form and sifting
5. psychological assessment
6. national assessment through exercises.

Candidates who are recommended after completing this selection process secure a place on the UCA training programme.

They must pass this to become a UCA.

2.8.3 Training programme

UCFs selected for advanced training undergo the National Undercover Advanced Training Programme. This modular training allows UCOs to be deployed in more complex investigations and infiltrations (with CPD to maintain their accreditation) based on their personal profiles, skills and ability.

Students require support from an identified mentor throughout the training programme. This mentor is provided by the home force or agency's undercover unit. The mentor will have received appropriate training and accreditation from the College of Policing.

The UCA training programme is made up of three phases:

- phase 1 – briefing
- phase 2 – formative
- phase 3 – assessment.

These phases include distance learning, ten weeks of mentoring and subject matter input. The course is competency-based with students assessed as competent or not.

UCOs will **not** be deployed in an advanced operational capacity (with the exception of those acting in supporting roles) until they have successfully completed the advanced training programme.

The College of Policing licenses all undercover training courses and accredits all who pass them. Undercover training is delivered to national standards by subject matter experts who hold an appropriate training qualification as recognised by the College.

3. Other roles

The undercover discipline has a number of important roles in addition to that of the undercover operative (UCO).

Main points:

- cover officers manage UCO security and welfare and interactions between UCOs and the operational team
- backstopping officers establish and maintain pseudo-identities for those who require them
- office managers manage the undercover unit's administrative systems
- COM-UCs (covert operations managers for undercover) are responsible for units and are key decision makers
- heads of unit are strategic managers for the undercover discipline
- operational leads run operations and set objectives and are unattached to units
- authorising officers authorise the use and conduct of UCOs
- senior responsible officers review the integrity, objectivity and legality of operations.

Contents

The College of Policing licenses all undercover training courses and accredits all who pass them. Undercover training is delivered to national standards by subject matter experts who hold an appropriate training qualification as recognised by the College.

3.1 Cover officer

The cover officer is an individual allocated to an undercover operation by the COM-UC. Cover officers are responsible for UCO security and welfare. They ensure interactions between the UCO and the operational team happen in accordance with agreed sterile corridor arrangements.

Cover officers are independent of the operational team and work under the direction of the undercover unit while undertaking cover officer duties. See section 29(5)(a)/29(4A)(a) of the Regulation of Investigatory Powers Act 2000 (RIPA).

Officers should have attended and passed the national cover officer course to undertake this role. Cover officers should be fully conversant with current law, procedures and guidelines relevant to undercover operations – this includes disclosure and revelation issues.

Where a UCO is donated by a law enforcement agency, the donor unit should allocate a cover officer to act as a conduit between the host cover officer and the donor unit. See the paragraph on host and donor units.

3.1.1 Checklist of responsibilities

In conjunction with the COM-UC, the cover officer:

- **makes sure** UCO welfare and security needs are met and documented
- **makes sure** there is proper oversight and management of UCOs and tactics
- **manages** UCOs on a day-to-day basis
- **makes sure** the deployment management record and other records are maintained throughout deployments in line with legislation, APP and standard operating procedures

- **makes sure** records are maintained throughout subsequent court proceedings and include any ongoing risk management and welfare considerations
- **maintains** the agreed sterile corridor between UCOs and certain members of the operational and prosecution teams as appropriate
- **liaises** with the operational lead
- **makes sure** the UCO's line manager is kept informed of the expected commitment
- **provides** updates on the UCO's welfare, deployment and any other relevant matters to the COM-UC, authorising officer and (where appropriate) the operational lead
- **makes sure** appropriate deconfliction processes exist – see the section on national databases
- **provides** tactical and operational advice to the operational team on all aspects of undercover deployments
- **makes sure** equipment is provided for operations (for example, recording and retrieval equipment, safety devices, communications equipment and vehicles)
- **makes sure** the UCO is fully proficient in all equipment used
- **makes sure** any failure to make a recording using technical equipment is documented together with the reasons why
- **advises** UCOs on creating audio and visual technical product
- **makes sure** operational expenditure is made available for the information and supervision of the operational lead
- **coaches and guides** UCOs to improve their performance and increase their resilience
- **makes sure** UCOs undertake continuing professional development.

3.2 Backstopping officer

The backstopping officer establishes and maintains pseudo-identities. These support and add credibility and authenticity to those who require them.

Pseudo-identities help preserve the true identity of a UCO and/or covert premises, maintain a UCO's legend and help minimise the risk of compromise.

Backstopping should be managed by a nominated person who is the single point of contact (SPOC) responsible for all backstopping issues. This role includes maintaining operational security in conjunction with the operational security officer.

3.2.1 Checklist of responsibilities

The backstopping officer:

- **manages and processes** all requests for backstopping and supporting documentation
- **acts** as the SPOC for the undercover unit
- **maintains** the undercover unit's covert infrastructure
- **makes sure** the level of backstopping is proportionate to the degree of scrutiny that can reasonably be expected to be encountered
- **makes sure** correct processes and procedures are adopted for all covert assets
- **assists and supports** the undercover unit's office manager
- **manages** the unit's vehicle fleet, including purchases and maintenance
- **assists** technical support staff with new technology and equipment purchases
- **maintains** records in support of all covert deployments and legend activity for auditing purposes and to provide integrity of any expenditure (including specific operational costs)
- **updates** the national undercover database
- **assists**, in conjunction with cover staff, with legend building/backstopping and UCO training, development and mentoring needs

- **makes sure** UCOs are conversant with legislation and practices that will have an impact on legend building
- **notifies** undercover unit members of any relevant changes to organisational policy and procedures that have taken place outside of undercover to make sure all members of the unit are aware of them and understand current practice.

3.3 Office manager

The undercover office manager is a designated individual who manages the undercover unit's administrative systems.

These systems support the covert nature of the unit and UCO deployments.

3.3.1 Checklist of responsibilities

The office manager may:

- **support** the unit's backstopping
- **maintain** records of monies issued to staff in support of UCO expenditure for deployments and legend building
- **be** a point of contact with other undercover units about administrative and financial matters that result from deployments between units
- **give** budgetary advice and recommendations to the head of unit and the COM-UC
- **be** the designated link between the undercover unit and the organisation's audit processes and procedures
- **maintain** the unit's human resources systems including records of vetting, training and attendance at psychological support meetings
- **notify** unit members of any relevant changes to organisational policy and procedure outside of the undercover discipline to help them remain current.

3.4 COM-UC

The COM-UC is an officer of at least inspector rank, or equivalent, who is responsible for an undercover unit (see RIPA section 29(5)(b) or Scottish equivalent).

The COM-UC is the decision maker regarding the covert tactics and tasking undertaken by UCOs. These decisions will be within the parameters of the authorisation granted by the authorising officer.

Officers should have attended COM-UC training to undertake this role.

3.4.1 Checklist of responsibilities

The COM-UC:

- **supports** the head of unit with the strategic direction and development of the undercover discipline
- **makes sure** consultation takes place with undercover units where the UCO will be deployed
- **manages** the tactical deployment and tasking of UCOs
- **makes sure** the operational lead is advised regarding undercover operations
- **provides** oversight and management of designated UCOs and tactics
- **maintains** covert structures, operational security and the security of assets and data
- **manages** staff vetting and the risks associated with access to covert facilities and information
- **makes sure** there is generic and operational health and safety risk assessment and psychological support – see the chapter on welfare
- **makes sure** accurate records are maintained and stored of:
    - everyone's working hours (including making sure that UCOs and cover officers are not fatigued)
    - operational disagreements involving the deployment of UCOs

  - the register of the issue, movement and return of UCO original notes
  - the deployment management record

- **manages** overseas UCO deployments
- **makes sure** briefings and debriefings are documented appropriately
- **receives** backstopping and legend building requests from undercover units
- **manages** legend building applications before they are presented to the approving officer for approval
- **assesses** UCOs according to the nationally agreed risk-based tenure policy
- **manages** updates to national databases
- **updates** national databases with details about UCO eligibility to deploy
- **makes sure** there is early consultation with prosecutors and subsequent liaison regarding witness anonymity
- **ensures** the safety and security of UCOs during proceedings
- **determines** (together with the operational lead) what intelligence from a deployment is passed to the confidential unit for dissemination as well as the handling requirement
- **liaises** (in conjunction with the operational lead) with the prosecutor or other bodies regarding disclosure of material from UCO operations which may have an impact on the safety or identification of the UCO and/or operational effectiveness.

Some COM-UC responsibilities may be delegated to the cover officer and some shared with the operational lead.

3.5 Head of unit

The head of an undercover unit is an officer of at least chief inspector rank or equivalent. They are responsible for the overall management, strategic direction and development of the undercover discipline.

Officers should have attended COM-UC training to undertake this role.

3.5.1 Checklist of responsibilities

The head of unit:

- **manages** covert structures, operational security and asset security
- **manages** staff vetting and the risks associated with access to covert facilities and information
- **makes sure** all appropriate risk assessments take place
- **makes sure** processes and procedures are in place to secure and maintain records held in the undercover unit
- **monitors** staff working hours
- **oversees** the effective and efficient management of resources
- **provides** independent oversight of recruitment, selection and training
- **has** ultimate control of unit finances
- **makes sure** the Code of Ethics is adhered to
- **has** overall responsibility for the welfare and wellbeing of all staff working for or on behalf of the unit
- **makes sure** there is effective internal and external stakeholder engagement
- **makes sure** there is a reintegration strategy to help undercover operatives return to other policing or agency duties.

3.6 Operational lead

The operational lead is an officer of at least inspector rank or equivalent. They are in charge of the undercover operation and set clear objectives for UCO deployments.

Before starting an operation the operational lead should consult the undercover unit and agree the approach. This is to make sure the approach fits operational objectives. The undercover unit will continue to help and give advice throughout the operation.

Operational leads should not be attached to the undercover unit nor be the line manager of deployed UCOs. They should be aware of current legal issues and guidelines relevant to undercover operations.

The identity of the operational lead and deputy must be recorded at all stages of the operation (see Statutory Instrument 2000/2725). Operational lead duties should be deputed only in exceptional circumstances.

3.6.1 Checklist of responsibilities

The operational lead:

- **makes sure** legislation is complied with
- **liaises** with the COM-UC and/or cover officer throughout operations and subsequent court proceedings
- **maintains** a sensitive policy/decision log
- **makes sure** there are sufficient resources to support the operation
- **makes sure** evidential material is prepared effectively and kept secure
- **sets** the operational objectives prior to deployment
- **makes sure** UCO original notes are maintained
- **makes sure** there is a record of unused material
- **makes sure** UCOs are briefed and debriefed appropriately
- **arranges** early consultation with the prosecutor at the appropriate level when a UCO deployment acquires material capable of being used in court as evidence
- **makes sure** (in consultation with the COM-UC and/or cover officer) that the authorising officer is notified at the earliest opportunity if there is a significant change in circumstances and/or it is intended to task the UCO in a significantly different way
- **ensures**, in conjunction with the cover officer, the security of the operation and all related correspondence and documentation in line with Government Security Classification requirements

- **liaises** with the COM-UC on any media strategy that may allude to undercover operations or have an impact on UCO security or welfare
- **makes sure** all relevant intelligence checks are made to support appropriate risk assessment
- **ensures** deconfliction of supporting and corroborating tactics
- **makes sure** regular reviews are submitted (at the direction of the authorising officer), including the reasons why executive action has not taken place
- **makes sure** annual authorisation renewals are submitted
- **makes sure** authorisation cancellations are submitted
- **determines** (together with the COM-UC) what intelligence from a deployment is passed to the confidential unit for dissemination as well as the handling requirement
- **liaises** (in conjunction with the COM-UC) with the prosecutor or other bodies regarding disclosure of material from UCO operations which may have an impact on the safety or identification of the UCO and/or operational effectiveness.

3.7 Authorising officer

The authorising officer is an officer of at least assistant chief constable rank or equivalent. They are responsible for authorising the use and conduct of UCOs.

Where it is likely that the use and conduct of any UCO will involve knowledge of legally privileged material or other confidential material being acquired, the relevant level of authorisation is increased to chief constable or equivalent.

Authorising officers should have attended and passed the College of Policing's authorising officer course prior to undertaking this role.

See also the chapter on authorisation and conduct.

3.7.1 Checklist of responsibilities

The authorising officer:

- **gives** written authorisations for each specified UCO
- **stipulates** the frequency of reviews
- **makes sure** designated roles are allocated to fulfil RIPA requirements
- **assesses** the adequacy of risk assessments and risk management relating to UCO deployment
- **records** their findings regarding collateral intrusion
- **makes sure** any intelligence opportunities that have not been acted on are documented and considered when deciding on continued authorisations
- **makes sure** the operational lead arranges early consultation with the prosecutor at the appropriate level where a prosecution is a likely outcome as a direct or indirect result of the UCO deployment.

3.8 Senior responsible officer

The senior responsible officer is a designated person in each organisation who is responsible for introducing and maintaining an internal review of the integrity, objectivity and lawfulness of undercover operations.

3.8.1 Checklist of responsibilities

The senior responsible officer:

- **ensures** the integrity of the public authority process for managing UCOs
- **ensures** compliance with Part II of RIPA and the CHIS Code of Practice (covert human intelligence sources)
- **makes sure** all records are kept available for inspection by the Office of Surveillance Commissioners (OSC)
- **oversees** the reporting of errors to the OSC
- **engages** with the OSC

- **implements** the OSC action plan
- **introduces and maintains** an internal review process which:
    - takes account of their unit's accreditation cycle
    - considers the types and frequency of operations
    - reviews foundation, advanced and online operations if they are conducted
    - uses sufficiently experienced senior officers who are independent of the operations
    - makes use of subject matter experts where required
    - employs a peer review where this is considered beneficial
    - considers the use of tactical parameters in operations in areas such as backstopping, welfare and cover and financial arrangements
- **makes sure** the review process is sufficient to ensure integrity, objectivity and compliance with the law.

4. Welfare

Undercover operatives (UCOs) require a safe, secure and confidential environment to receive psychological assessment and mental wellbeing support from qualified practitioners.

Main points:

- personality and psychological assessments feature in UCO selection, training and retention
- UCOs receive psychological assessment and mental wellbeing support from qualified practitioners
- practitioners will respect UCO confidentiality but report serious concerns to the relevant force or agency
- COM-UCs (covert operations managers for undercover) are responsible for UCO welfare arrangements
- undercover units should have a formal system for assessment and support
- host and donor units need to cooperate to ensure UCO security and welfare.

Contents

4.1 Assessments

There are two types of UCO assessment:

- personality assessment
- psychological assessment.

4.1.1 Personality assessment

Candidates going through the foundation programme undergo a personality assessment with an occupational psychologist who is approved by the College of Policing. This assessment helps identify the personal characteristics relevant to the requirements of the role.

The personality assessment evaluates a candidate's motivation, suitability and resilience for the UCO role. It does this by identifying areas of strength and potential areas of concern that may require further exploration during the assessment process.

The 16PF (Sixteen Personality Factor Questionnaire) and NEO PI-R (Neuroticism-Extraversion-Openness Personality Inventory-Revised) tests are used in the personality assessment.

4.1.2 Psychological assessment

Candidates going through the advanced programme undergo a psychological assessment. It is a semi-structured one-to-one interview session with a qualified practitioner (for example, a chartered clinical psychologist or registered psychiatrist).

This assessment ascertains whether there are any psychological factors that may present a risk to the candidate's wellbeing, their performance in training or their suitability to undertake advanced work. It also identifies positive factors indicating suitability for deployment.

Following the psychological assessment a brief report is produced by the practitioner for the advanced selection assessment centre panel.

4.1.3 Ongoing assessments

Active UCOs are subject to ongoing psychological assessment as follows:

- undercover foundation operatives (UCFs) – at the direction of the relevant COM-UC
- undercover advanced operatives (UCAs) – at least every six months and at the start and end of significant deployments if these do not coincide with scheduled appointments.

Ongoing assessments are carried out by a College-approved psychologist and may ascertain whether there are any psychological factors that may present a risk to the UCO's wellbeing or to the effectiveness and safety of any operation on which the UCO may be deployed.

Ongoing assessments also measure the presence of positive factors indicating suitability for particular deployments.

Consideration should be given to the potential psychological impact that frequently viewing graphic and disturbing images can have on undercover online operatives. This will be addressed and managed by an approved psychologist.

4.2 Practitioners

Practitioners will be chartered clinical psychologists registered with the Health & Care Professions Council or psychiatrists registered with the General Medical Council.

They should have at least five years' relevant post-qualification experience including specific experience of assessments in high-risk occupational contexts. All practitioners should be vetted to SC (security check) level.

Practitioners:

- **work** with the COM-UC (and other personnel as appropriate) to ensure the most effective and accurate psychological assessment of the UCO and the most effective support and treatment, where appropriate
- **give** written and verbal reports to the COM-UC to help with decisions about UCO deployments

- **provide** appropriate guidance on resilience and coping strategies to prevent psychological crises or ill health from developing
- **make** recommendations for support or treatment as appropriate, in consultation with the COM-UC and appropriate wellbeing support providers.

4.3 Confidentiality

UCOs should be made aware that practitioners are obliged to inform the relevant undercover unit, force or agency if they have serious concerns about the wellbeing or safety of the UCO, other staff or members of the public, or about the ethics or legality of UCO activities.

This policy is in line with the UCO code of conduct which requires UCOs to take personal responsibility for maintaining their mental wellbeing and informing managers of anything which may have an impact on their fitness to operate.

4.4 Support

Mental wellbeing support is the therapy or treatment that may be recommended following psychological assessment. The purpose of such support is to address any psychological difficulties the UCO may be experiencing and provide an up-to-date record for the COM-UC.

Practitioners who provide this support function may come from a wider range of professional backgrounds (for example, counsellors or cognitive behavioural therapy specialists). They should, however, be registered and accredited by an appropriate professional body and vetted to SC level.

Practitioners who provide the psychological assessment function may also provide a mental wellbeing support function (if they are suitably qualified), but they should **not** do so for the same UCO. This is to prevent a conflict of interest whereby the person recommending treatment is also the person providing that treatment.

4.5 Formal system

COM-UCs are responsible for the arrangements for the psychological assessment and mental wellbeing support of UCOs.

Every undercover unit should have a formal system for assessment and support that:

- **provides** assessments by suitably qualified and experienced practitioners
- **makes sure** assessment providers have a contract and clearly defined terms of reference covering the purpose, approach, outcomes, referrals and arrangements for the security of records
- **provides** a defined, confidential reporting mechanism to highlight issues of concern and grounds for withdrawing staff from operations
- **provides** a mechanism for the COM-UC to feed concerns about UCOs to the psychologist/psychiatrist and vice versa
- **makes sure** other undercover unit staff are subject to psychological assessment and mental wellbeing support as necessary
- **creates** a climate that supports openness, honesty and positive regard for UCO wellbeing
- **provides** leadership that creates a culture where seeking internal and external support is regarded positively and is not a barrier to seeking care services
- **makes sure** local policies underpin wellbeing and psychological support where appropriate
- **monitors** the effectiveness of UCOs and cover officers, both as individuals and as a partnership
- **makes sure** there are appropriate protocols and policies for creating the right conditions to support UCO wellbeing (for example, that consider periods between deployments and ensure there are exit strategies)
- **makes sure** procedures exist for self-referral, required referral and routine psychological assessment with practitioners

- **makes** decisions about which deployments are particularly demanding or especially psychologically challenging and, therefore, require more frequent psychological assessments
- **maintains** working relationships with practitioners to ensure effective briefing and debriefing and sharing of concerns, while maintaining appropriate confidentiality
- **makes sure** operatives have clarity on and plans for returning to other policing or agency duties
- **makes sure** everyone complies with mandatory support and assessment requirements and that appropriate records are kept.

4.6 Host and donor units

The **host** undercover unit is the unit which supports the operational lead and investigation team in providing undercover tactics. Sometimes UCOs are donated from other undercover units to support operations. In such cases the donating UCO's undercover unit is referred to as the **donor** unit.

The cover officer in the host unit conducts baseline assessments and ongoing reviews with all UCOs to assess their performance and wellbeing. The host cover officer maintains regular contact with the donor cover officer regarding the UCO's security and welfare. If there is cause for concern and either cover officer believes that the UCO requires psychological assessment, this will be arranged via the donor COM-UC.

Where a COM-UC in the host unit has a concern about a UCO and wishes to make a referral for psychological assessment, they should arrange this via the COM-UC of the donor unit.

The content of the psychological assessment report will be considered by the donor unit COM-UC. It will inform the decision made by the donor and host COM-UCs as to whether the UCO will be allowed to continue with their deployment.

If mental wellbeing support is required (for example, counselling), this will be provided by the donor COM-UC using qualified practitioners. The donor COM-UC is responsible for making sure that all UCAs attend ongoing psychological assessments, as appropriate.

5. Backstopping and legend building

Backstopping and legend building are mutually supportive processes designed to develop, maintain and support covert identities and structures capable of withstanding scrutiny.

Main points:

- all undercover operatives (UCOs) and some support staff require an appropriate level of backstopping
- all backstopping should be approved by the head of unit and processed via a backstopping officer
- support provisions should be fit for purpose and there are policies for having covert documents
- initial planning for legend building should include contacting the local undercover unit
- some legend building activity may not require authorisation but be subject to an approval process
- legend building should not be a precursor to authorised operations
- UCOs and cover officers have responsibilities where legend building obtains evidence and/or intelligence
- there are UK single points of contact (SPOCs) for international considerations.

Contents

5.1 Backstopping: purpose and process

Backstopping is the process of establishing and maintaining documentation and facilities that support covert identities and structures capable of withstanding scrutiny.

Backstopping enhances the security of a UCO and/or covert premises and reduces the risk of exposure.

All UCOs, COM-UCs (covert operations managers for undercover), cover officers and some support staff require a level of covert backstopping commensurate with the role they are expected to perform.

All requests for backstopping and supporting documentation should be approved by a superintendent or equivalent and processed via the undercover unit's backstopping officer.

5.2 Backstopping: support provisions

Undercover support provisions should:

- **be** fully backstopped, with no reference to law enforcement activity
- **include** premises that are fit for purpose with:
    - protocols for visitors
    - external security
    - no external identifiers
    - secure communications
- **provide** sufficient backstopping for UCOs to effectively service their needs in-role
- **make sure** there are fully supported and up-to-date legends that can withstand intrusive scrutiny
- **include** business continuity plans.

5.3 Backstopping: covert documents

All UCOs, COM-UCs, cover officers and some support staff should have covert documentation commensurate with their needs.

Unless in exceptional circumstances, staff should **not** have more than one set of documentation in their physical possession. This is to prevent the risk of compromise.

Covert documentation should be issued and stored in accordance with local procedures when not being used.

5.4 Legend building: initial planning

Legend building is the process of visiting or frequenting locations to develop and maintain a covert identity where there is no intention to acquire intelligence or evidence or engage with the subjects of an investigation or operation.

Undercover advanced operatives (UCAs) routinely engage in legend building – undercover foundation operatives (UCFs) less so.

Initial planning should involve contacting the relevant undercover unit(s) where appropriate. This is to understand any particular sensitivities in the local community where the UCO is to conduct legend building activity and be aware of similar activities being undertaken by other public authorities which could have an impact on the legend building. It is the responsibility of the COM-UC to do this.

Contact should always be made with the undercover unit in the Police Service of Northern Ireland when planning to legend build in Northern Ireland.

5.5 Legend building: approval not to authorise

The Office of Surveillance Commissioners has acknowledged that some legend building activity, where the criteria for an authorisation under the Regulation of Investigatory Powers Act 2000 (RIPA) are not met, may not require authorisation. In these cases an ‘approval’ not to authorise must be obtained.

The decision not to authorise, and the responsibility to record the rationale, rests with the authorising officer (assistant chief constable or equivalent) who would have granted authorisation had it been deemed appropriate. The decision not to authorise should be reviewed at least every 12 weeks. As approval is not part of RIPA, the requirements of Statutory Instrument 2000/2725 will not apply.

Requests for legend building activity should be reviewed by the COM-UC before they are presented to the approving officer. The COM-UC should be satisfied that:

- the legend building plan is necessary and proportionate
- collateral intrusion has been and continues to be considered.

If legend building activity exceeds or is likely to exceed 12 months, approval remains with the approving officer at assistant chief constable level or equivalent. Legend building approvals should be reviewed at the direction of the approving officer, but the review period should not exceed three months.

There are forms for approving legend building activity and forms for reviewing or cancelling legend building activity.

5.6 Legend building: evidence and intelligence

Prior to deployment, cover officers should make sure that UCOs undertaking legend building activity understand that they may be required to give evidence in court if they obtain any evidence during deployments.

If incidental intelligence is acquired the cover officer is responsible for sanitising and disseminating it through the confidential unit or equivalent. Original notes of the circumstances should be maintained to an evidential standard.

5.7 Legend building: international considerations

The International Working Group and the European Cooperation Group facilitate cooperation between undercover units in the UK and overseas. The UK is represented on both groups by SPOCs

from the National Crime Agency and the Metropolitan Police Service.

Where UCOs are physically deployed outside the UK to undertake legend building activity, advice should be sought from a senior member of staff in the relevant overseas undercover agency after consulting one of the UK SPOCs. Approval for UCFs to engage in legend building activity outside the UK will be given only in exceptional circumstances.

Foreign UCOs wishing to legend build in the UK should seek advice from the head of unit in the relevant UK agency via one of the UK SPOCs. This ensures UK and international legislation and protocols are complied with.

Her Majesty's Revenue and Customs has separate arrangements with overseas partners.

6. Operational security

Secure systems are critical to the integrity of the undercover unit, its staff and operations.

Main points:

- the COM-UC (covert operations manager for undercover) is in charge of overall security and others have specific and/or general security responsibilities
- undercover unit staff should be vetted to at least SC (security check) level, as should some external associates
- there are structures and processes for dealing with intelligence from sensitive sources
- there are national databases to help identify risk and deconfliction and reduce the risk of compromise
- freedom of information and data protection requests should be reported to a national office before they are responded to
- covert strategies need a media policy and the COM-UC should agree all undercover media references
- social media can undermine and compromise covert resources, assets and activity.

Contents

6.1 Security responsibilities

The COM-UC is responsible for overall security, but all staff have a role to play in identifying security issues and adhering to security policies.

The operational security of the undercover unit, including its interactions with the operational team, is achieved and maintained by:

- **making sure** all staff undergo appropriate vetting
- **making sure** all identified risks are assessed and documented and that there are appropriate risk management measures – this requires consultation with an operational security officer
- **preserving** the sterile corridor/firewall
- **using** and managing confidentiality agreements – see an example agreement for all staff and an example agreement for undercover operatives (UCOs)
- **managing** asset security, including IT security
- **applying** Government Security Classification requirements
- **making sure** psychologists' confidential records are stored securely with controlled access in line with College of Policing guidance to psychologists
- **ensuring** deconfliction of operations – the cover officer is responsible for this
- **referring** and reporting to national databases as appropriate
- **ensuring** liaison with local or regional freedom of information (FOI) teams and coordinating responses to FOI requests nationally
- **having** a media policy that does not expose covert techniques
- **restricting** awareness of sensitive sources and covert methods on a need-to-know basis
- **briefing** the operational lead on the need to protect covert methods and terminology used with the media and in prosecution reports (this briefing takes place before the undercover operation starts)

- **making sure** audio/visual product and other evidential material is managed safely
- **adhering** to national protocols on handling, copying and using audio/visual product and other evidential material in any prosecution case.

6.2 Vetting

Undercover unit personnel should be security vetted to at least SC or MV (management vetting) level. Heads of units, COM-UCs and psychologists should hold a minimum of SC clearance.

6.3 Sensitive source intelligence

Intelligence from sensitive sources should be managed securely, suitably sanitised and graded properly for dissemination using an intelligence report.

The operational lead should make sure that sterile corridors are established and maintained for receiving such intelligence. They will consult the confidential unit and cover officer.

Memoranda of understanding should be used between relevant parties where appropriate.

6.4 National databases

There are two national databases that contain details of UCOs and deployments:

- **national undercover database** (NUD) – provides a centralised repository of all UK UCO deployments and legend building activity to improve safety and enhance operational deconfliction
- **national index** – holds the personal details of all UK UCOs including their training history and skills profile.

Undercover units should submit pre-authorisation check forms to the NUD so that checks can be conducted in the database and other datasets to identify risk and deconfliction. Units should also continue to submit updates to identify and reduce the risk of

compromise to the operation and UCOs. An operational conclusion report should be submitted to the NUD at the end of the operation.

The NUD consists primarily of areas that have been directly subject to undercover tactics, including:

- people
- organisations
- locations
- events.

6.5 Freedom of information and data protection requests

Responsibility for responding to FOI and data protection requests lies with the receiving force or agency. Before responding, however, forces/agencies should report all requests to the National Police Freedom of Information and Data Protection Unit (NPFDU) as soon as possible.

The NPFDU manages requests on behalf of the National Police Chiefs' Council (NPCC), who maintain communication with the National Undercover Working Group (NUWG).

The NUWG maintains FOI details to ensure the undercover community is aware of any themed requests.

6.6 Media policy

The use of UCOs should be subject to a media policy to protect covert assets from media exposure. This policy should state that no information will be passed to the media that might lead to any of the following (even if they have been referred to in court or elsewhere in the public domain):

- identification of UCOs or covert human intelligence sources (CHIS)
- revelation of covert tactics, techniques or methods
- revelation of the existence or details of particular items of technical equipment

- disclosure of any other sensitive process or procedure.

Despite various publications and television programmes describing covert tactics, law enforcement agencies should not endorse exposure.

There may be cases where it is deemed beneficial to reference the use of UCOs in media releases. This should be agreed by the COM-UC on a case-by-case basis.

Formal requests from television or film companies or other organisations to take part in fly-on-the-wall type programmes depicting the use of undercover techniques should be referred to the NUWG.

6.6.1 Neither confirm nor deny

The established principle of neither confirm nor deny (NCND) is used by law enforcement agencies to protect covert methods, sensitive information and the identity of sources of information including UCOs.

NCND is not used to hide information that the force or agency does not wish to disclose. Rather, it safeguards tactics and the lives and wellbeing of UCOs, their families and others.

Sometimes simply confirming or denying whether a force or agency holds a particular category of information could itself disclose sensitive and damaging information. The principle of NCND is needed to prevent harm which may arise if law enforcement agencies have to confirm or deny whether they hold particular information. Specifically:

- to confirm that a person is a UCO would place that person in immediate and obvious danger
- to deny that a person is a UCO may place another person in immediate and obvious danger
- to comment either way in one case raises a clear inference where there is a refusal to comment in another case that there is something to hide in that case.

The local police force or law enforcement agency communications office can help handle media enquiries. In cases of difficulty the NPCC media office can advise. See also the NCND report.

6.7 Social media

All undercover unit staff should be aware of the dangers posed through exposure in true identity on social media networks, as this may undermine the covert nature of their role.

Any individual who compromises themselves, colleagues, operations or covert assets by using social media may be subject to disciplinary procedures. Any exposure will be subject to a thorough risk assessment.

7. Authorisation and conduct

The use and conduct of an undercover operative (UCO), when regarded as a sensitive source, is subject to individual authorisation under the Regulation of Investigatory Powers Act 2000 (RIPA).

Main points:

- authorisations must have due regard to legislation and case law
- authorisations, documentation and notifications are managed in accordance with set processes
- collateral intrusion must be reasonable and justified in the specific circumstances
- there are procedures for reviewing, renewing and cancelling authorisations
- there are provisions for authorising multiple operatives, operatives from foreign agencies and overseas deployments
- UCOs remain bound by the laws, rules and regulations governing the respective law enforcement agencies
- authorisations should make the parameters of UCO conduct clear and not include certain kinds of conduct.

Contents

7.1 Authorisation

Authorisations must have due regard to RIPA (and any other relevant legislation), the CHIS Code of Practice and case law.

The COM-UC (covert operations manager for undercover) is responsible for making sure (together with the operational lead) that operational and personal risk assessments have been completed before any authorisation or approval is considered.

Forms for authorisations, reviews, renewals and cancellations may be submitted to the authorising officer by way of an electronic system or in hard copy. All records relating to authorisation processes must be retained.

7.2 Authorisation: applicant and applications

The role of the applicant is to present the application for a use and conduct authorisation to the authorising officer. The applicant will outline clearly the information or intelligence on which the application has been made. This helps the authorising officer reach a decision.

Each application should be accompanied by a personal risk assessment for each UCO.

UCOs should be individually identified from the outset by their national index number.

7.2.1 Application documents

Application documents should include:

- an application for an authorisation
- a risk assessment for each operative to be deployed
- an authorisation or refusal
- oral application and authorisation, where appropriate
- a minute sheet.

Also consider including:

- any appropriate comments from the Office of Surveillance Commissioners (OSC)

- advice from the prosecutor, if appropriate
- a letter of request, if appropriate (overseas).

Applicants should be aware that when completing an authorisation, they are seeking an authorisation for the deployment of a UCO(s) and **not** for an operation.

7.3 Authorisation: authorising officer and authorisations

Authorising officers (AOs) are independent of investigations, of the appropriate rank (or grade equivalent) and have completed accredited training. See annex B of the CHIS code for a table of authorisation levels.

All undercover authorisations (foundation or advanced) require authorisation at assistant chief constable rank or equivalent for 12 months. **The exceptions to this are urgent and higher authorisations, which are described below.**

The OSC must be notified of all authorisations within seven working days.

7.3.1 Urgent oral authorisations

In urgent cases where it is not practical for the application to be considered by an assistant chief constable or equivalent, oral authorisation may be given by a RIPA AO-trained superintendent or equivalent.

Urgent oral authorisations last for no more than 72 hours, at the conclusion of which a cancellation or renewal must have been submitted, as appropriate.

7.3.2 Higher authorisations

The authorising officer must be at chief constable rank or equivalent (senior authorising officer), where one of the following applies:

- an existing authorisation will, or is believed likely to, exceed 12 months (long term, see Statutory Instrument 2013/2788)
- an authorisation is intended, or likely, to acquire legally privileged material or other confidential information – **in this**

case the relevant period of authorisation is three months.

The OSC must give prior approval, and the authorisation comes into effect once this is acknowledged by the senior authorising officer.

If a UCO has not been authorised on the same investigation or operation for at least three years, any previous authorisations will be disregarded for the purposes of calculating the above periods.

7.4 Authorisation: collateral intrusion

The authorising officer should take into account the risk of interfering with the private and family life of persons who are not the intended subject of the UCO's activity.

Collateral intrusion must be reasonable and justified in the specific circumstances. The mitigation of all forms of collateral intrusion should be planned for and considered.

Consideration should be given to two categories of collateral intrusion:

- **unavoidable** – collateral intrusion (including details of any measures taken to limit it and why the intrusion is justified) should be kept to the minimum necessary to achieve operational objectives
- **potential** – other collateral intrusion (including details of any measures taken to limit it and why the intrusion is justified).

Where UCO activity is deliberately proposed against individuals who are not suspected of direct involvement in the investigation, interference with their private and family life should not be considered as collateral intrusion but, rather, as intended intrusion and authorised as appropriate.

7.5 Authorisation: reviews

Regular reviews, as determined by the authorising officer, are required to update the authorising officer on any change in

circumstances, impact on the necessity and proportionality of the activity and UCO security and welfare.

The requirement for reviews is set out in sections 3.12 to 3.16 and in sections 5.16 and 5.17 of the CHIS code.

If the original authorisation identifies a likelihood of a future need for additional UCOs, these can be authorised at the time of the review if the authorising officer considers the statutory requirements to be met.

7.5.1 Review documents

Review documents are made up of:

- the authorisation
- a review document
- an updated risk assessment, if appropriate.

7.6 Authorisation: renewals

All renewals other than following urgent oral authorisation require authorisation at chief constable rank or equivalent, with prior OSC approval (see Statutory Instrument 2013/2788).

7.6.1 Renewal documents

Renewal documents should include:

- an application for the renewal
- a risk assessment for each operative to be deployed
- an authorisation or refusal
- oral application and authorisation, where appropriate
- a minute sheet.

Also consider including:

- any appropriate OSC comments
- advice from the prosecutor, if appropriate
- a letter of request, if appropriate (overseas).

7.6.2 Nine months

Where an authorisation will, or is believed likely to, exceed 12 months a notification form must be sent to the OSC at the nine-month point. Where a UCO is deployed beyond the nine-month stage but a renewal will not be sought at 12 months the OSC should be informed.

The OSC requires the following information:

- name of the law enforcement agency concerned
- operation name
- UCO number
- current authorisation start and expiry dates
- nine-month date
- the location where all associated paperwork can be inspected
- details of a single point of contact (SPOC) for the surveillance inspector.

Following receipt of the nine-month notification form, a surveillance inspector will be identified to undertake a detailed inspection of all necessary authorisation records.

The surveillance inspector will produce a report for the surveillance commissioner in advance of the formal renewal request from the law enforcement agency. This report will subsequently be sent from the OSC to the senior authorising officer in the relevant law enforcement agency who is responsible for considering the renewal.

7.6.3 Eleven months

The senior authorising officer should consider the renewal at the 11-month stage. This is to allow sufficient time for the OSC to consider whether to grant prior approval and allow time for any further clarification within the 12-month period.

If prior approval is granted, the renewal becomes effective on the date when the original authorisation would otherwise have expired.

7.6.4 Missed renewals

If the need for a prior approval renewal has been overlooked, the law enforcement agency may need to cancel the UCO's use and conduct at the end of the long-term authorisation (if it has not already been exceeded) and seek prompt and fresh authorisation under the prior approval arrangements.

It should not be assumed that a surveillance commissioner will be able or minded to deal with any such oversight outside of the usual arrangements detailed above.

During the intervening period the UCO should not be deployed. Where circumstances demand that they have contact with subjects (for reasons of safety or to deal with a situation involving risk to life or the serious jeopardy of the operation), the senior authorising officer should consider whether an emergency authorisation lasting 72 hours should be granted.

In all cases where a prior approval has been overlooked, the OSC must be informed at the earliest opportunity and advised of the remedial action taken.

7.7 Authorisation: cancellations

There are two stages to the cancellation process:

1. cancellation by the authorising officer
2. notifying the OSC.

An application for cancellation and the personal risk assessment must be presented to the authorising officer.

For any UCO activity which was likely to obtain legally privileged material or confidential information, the commissioner will expect to be informed whether such material or information has been obtained and, if so, what steps have been taken to deal with it.

7.7.1 Cancellation documents

Cancellation documents are made up of:

- an application to cancel
- an authorisation to cancel
- a risk assessment, if appropriate

- an OSC cancellation notification form.

7.8 Authorisation: multiple operatives

A single authorisation may be used to authorise more than one UCO, provided operatives are individually identified. The application should set out the necessity and proportionality of using multiple UCOs and specify their individual use and conduct.

Each UCO will be authorised for 12 months. Notifications at nine months and renewal times are particular to each individual UCO's authorisation.

UCOs may be introduced or removed from the existing authorisation at the time of review. The risk assessment should be updated.

7.9 Authorisation: operatives from foreign agencies

Operatives from foreign law enforcement agencies may be authorised under RIPA to support domestic and international investigations or operations.

Consideration should be given to authorising operatives from foreign agencies at the level prescribed by Statutory Instrument 2013/2788, as if the individuals hold an office, rank or position with an organisation listed in the order. See section 4.31 in the CHIS code.

7.10 Authorisation: overseas deployments

Operatives from UK law enforcement agencies may be authorised under RIPA for overseas deployments.

See also the section on international considerations for legend building activity.

7.11 Conduct

UCOs remain bound by the laws, rules and regulations governing the respective law enforcement agencies.

Authorisations should not include any conduct likely to have a negative impact on the health and wellbeing of UCOs, nor should UCOs undertake conduct that could have such consequences.

Neither should authorisations allow any activity that could have a negative impact on the reputation of undercover policing or law enforcement.

While an activity may not, in itself, be considered to have a negative impact, the cumulative effect should be considered and managed.

7.12 Conduct: sexual relationships and sexual activity

It is never acceptable for a UCO to form an intimate sexual relationship with those they are employed to infiltrate and target or may encounter during their deployment. This conduct will never be authorised, nor must it ever be used as a tactic of a deployment.

The civil case of DIL v MPC 2014 EWHC 2184 (QB) resulted in substantial compensation payments and the public naming of two former UCOs. It was acknowledged that long-term sexual relationships are never acceptable in undercover policing, a position also stated in a report from Operation Herne by Chief Constable Mick Creedon (March 2014).

Conduct may be authorised that involves **communications** of a sexual nature (for example, online) where the authorising officer believes it is necessary and proportionate to operational objectives. The parameters of the conduct must be considered and set by the authorising officer, and will be subject to regular and careful review.

If a UCO engages in unauthorised sexual activity for whatever reason (for example, they perceive an immediate threat to themselves and/or others if they do not do so) this activity will be restricted to the minimum conduct necessary to mitigate the threat. In such extreme circumstances UCOs **must** record and report this to the cover officer at the earliest opportunity. The authorising officer will be informed immediately and the

circumstances investigated for welfare and training purposes, potential breaches of discipline or criminal offences and to allow an appraisal of the operation.

7.13 Conduct: controlled drugs

The taking of controlled drugs by a UCO will not be authorised as a tactic of a deployment.

If a UCO takes controlled drugs because they perceive an immediate threat to themselves and/or others if they do not do so, this should be restricted to the minimum extent necessary to mitigate the threat. They **must** record and report this to the cover officer at the earliest opportunity so that the:

- operative can receive medical attention
- authorising officer is informed
- circumstances can be investigated for welfare and training purposes, potential breaches of discipline or criminal offences and to allow an appraisal of the operation.

7.14 Conduct: participation in criminal activity

For an undercover deployment to be effective it may be necessary for the UCO(s) to participate in the criminal activity about which they have been tasked to report. Case law has recognised the use of UCOs to participate in criminal activity and has identified the limits of acceptable law enforcement conduct (R v Loosely [2001] UKHL 53). This will be granted as part of the conduct specified in the RIPA authorisation.

7.14.1 Authorising officer considerations

Authorising officer considerations in granting such an authorisation include that UCO(s):

- do not actively engage in planning and committing the crime
- are intended to play only a minor role
- participate only where essential to enable law enforcement to frustrate the principal criminals and arrest them (albeit for lesser offences such as attempt or conspiracy to commit crime, or carrying offensive weapons)

before injury is done to any person or serious damage is done to property.

7.15 Conduct: agent provocateur

Agent provocateur has been defined as a person who entices another to commit an express breach of the law which they would not otherwise have committed and then proceeds to inform against them in respect of such an offence.

Case law has established that conduct by UCOs which does no more than present the subject(s) of the operation with an unexceptional opportunity to commit a crime which they would have committed with another is perfectly acceptable (R v Loosely [2001] UKHL 53). However, the UCO must not instigate the commission of a crime which would not otherwise have been committed with somebody else.

7.16 Conduct: parameters

The authorisation should make clear the precise parameters of the UCO's conduct and operatives should acknowledge these when briefed. Authorised conduct may differ between UCOs. The cover officer, COM-UC and operational lead will ensure that specific tasking of operatives remains within the parameters of the authorised conduct.

Where fresh tasking in pursuit of operational objectives is being contemplated, the applicant and authorising officer should consider whether the proposed tasking is outside the authorised conduct. If it is, the matter should be dealt with by way of a review.

8. Planning, risk and deployment

Undercover units do not initiate undercover operations but are central to their planning, risk assessment and deployment.

Main points:

- all undercover deployments should be planned in consultation with the undercover unit
- operational and personal risk assessments should be conducted and kept under constant review
- there are pre-deployment responsibilities, deployment responsibilities and post-deployment responsibilities
- technical resources are available via the undercover unit and there should be an agreed technical policy
- consultation with the prosecutor should take place at appropriate times and include appropriate staff.

Contents

8.1 Planning

Operational leads should liaise with the undercover unit whenever an undercover deployment is being considered. This allows operational leads to consider the overall circumstances of their operation and the requirement for and proportionality of covert tactics and methods.

Undercover unit staff will expect a presentation (usually only oral in the early stage) about the planned or ongoing investigation or the particular law enforcement problem. This offers an initial opportunity for undercover staff to consider tactical options. The unit will often identify a single point of contact (SPOC) to provide undercover tactical advice for the potential operation.

The operational lead for any prospective undercover activity should be able to demonstrate to the undercover unit and the authorising officer that the tactic is supported by the law enforcement agency's tasking regime.

The operational lead should start a sensitive policy/decision log to help protect undercover tactics.

8.1.1 Initial planning

Initial planning should involve contacting the relevant undercover unit(s) where appropriate. This is to understand any particular sensitivities in the local community where an undercover operative (UCO) is to be deployed and be aware of similar activities being undertaken by other public authorities which could have an impact on the deployment. It is the responsibility of the COM-UC (covert operations manager for undercover) to do this.

Contact should always be made with the undercover unit in the Police Service of Northern Ireland when planning to operate in Northern Ireland.

Initial planning should also consider the possible need for increased resources over time. It can be as damaging to the undercover tactic to prematurely halt an operation for lack of resources as it can be to suffer a compromise. The operational lead and undercover unit need to show that they have considered resource implications beyond initial deployment.

The undercover unit should be able to provide sufficient personnel and equipment to safely achieve the objective(s) of the

deployment. The operational team should be able to provide all the required investigative support to the deployment.

All decisions made in respect of undercover activity should adhere to national decision model principles and comply with National Undercover Working Group (NUWG) standard operating procedures.

8.1.2 Assessing options

All options should be assessed before commencing deployment. If undercover unit staff are satisfied that an undercover deployment appears appropriate, they will consider the extensive range of tactics available to UCOs.

Given the frequent and detailed scrutiny of policy and decision logs at legal proceedings, the operational lead will likely require an overview of:

- tactics considered
- tactics discounted, including rationale
- favourable tactics, including rationale
- tactics to deploy to best achieve the operational objective(s).

8.1.3 Making decisions

The decision as to which tactics to deploy should be made by the operational lead in consultation with the undercover unit.

If there is a conflict between the operational lead and the undercover unit (for example, over operational objectives, specific tactics, UCO safety or media issues), the head of unit should refer the matter to the person with overall responsibility for the undercover discipline in the force or agency.

8.2 Risk assessment

Risk assessments should be kept under constant review throughout deployments.

8.2.1 Operational risk assessment

Operational risks associated with proposed deployments should be addressed in the application for authorisation.

Examples include:

- community issues
- reputational risks
- risks to members of the public.

The operational lead, in conjunction with the COM-UC, is responsible for making sure that the operational risk assessment is completed and maintained throughout the operation.

8.2.2 Personal risk assessment

A personal risk assessment must be completed for each UCO deployed. This assessment deals with specific risks to the UCO(s), for example, skills and knowledge.

The COM-UC, in conjunction with the cover officer, is responsible for making sure that personal risk assessments are completed and reviewed throughout the operation.

UCOs need to be aware of additional health and safety risk assessments covering generic issues such as:

- safe handling of firearms
- arrest procedures
- needle stick injuries.

8.3 Pre-deployment responsibilities

Prior to deployment, the operational lead and cover officer should make sure that all UCOs:

- receive instructions
- understand the use and conduct of the authorisation
- are briefed on the deployment.

The operational lead (or their deputy) should read the instructions

to UCOs to the operatives at the start of the operation. A record of this should be made in the deployment management record (DMR).

The operational lead should make sure that UCOs are regularly reminded of the instructions throughout the operation, as appropriate. Once a deployment has begun, the cover officer should make sure requirements outlined in the DMR are complied with.

The operational lead (in conjunction with undercover unit staff) is also responsible for:

- legislative compliance
- setting clear operational objectives
- setting the deployment tasking for UCOs
- logistical support.

8.3.1 Substance misuse testing

Every member of a law enforcement agency is subject to their force or agency's substance misuse testing policy. In addition, due to the role UCOs perform, every undercover unit should have a random substance misuse testing policy for UCOs. See also the section on controlled drugs.

Where UCOs are donated from another unit, the host undercover unit's policy and procedures will apply **in addition** to those of the donor undercover unit. See the section on host and donor units.

8.4 Deployment responsibilities

8.4.1 Briefings and debriefings

The initial briefing is where all relevant parties meet and officially commence an undercover deployment. Subsequent briefings and debriefings will take place as necessary. Briefings should be documented in the DMR.

The cover officer should attend every operational briefing and debriefing. This is so that they can:

- manage UCO welfare and security

- make certain that evidence, intelligence and information is recorded correctly
- advise the operational lead and the operational team about tactical options.

Concerns which are not addressed in briefings and debriefings should be brought to the attention of the COM-UC.

See also APP on briefing and debriefing.

8.4.2 Attendance

The occasional absence of an operational lead (or deputy) may be unavoidable. The cover officer should make sure, however, that briefings and debriefings are not further deputed to other members of the operational team on a regular basis.

The cover officer should try to make sure briefings and debriefings are attended by the operational lead/deputy and appropriate members of the operational team (for example, exhibit and disclosure officers and, where appropriate, a representative from the confidential unit).

8.4.3 Working hours

Those involved in undercover deployments must consider the Working Time (Amendment) Regulations 2003 and remain subject to legislation and the regulations and rules governing the respective law enforcement agencies.

The cover officer and UCO should make sure they are not mentally or physically fatigued while deployed on operations. The nature of undercover operational activity is unpredictable. The COM-UC or operational lead should regularly review the hours worked and the impact this is having on the UCO, the cover officer and the operation.

UCOs and the cover officer should inform the COM-UC or operational lead if they are suffering from mental or physical fatigue. The COM-UC should make sure UCO and cover officer working hours are recorded accurately.

8.5 Post-deployment responsibilities

The need to protect UCOs continues after cancellation of the use and conduct authorisations (see sections 5.29 and 6.14 of the CHIS Code of Practice). Items which could compromise the identity of UCOs should not be disclosed (for example, for training purposes) without prior agreement from the undercover unit.

8.5.1 Compromise and exposure

The cover officer should report any exposure or compromise of covert methods and tactics to the national compromise database and national undercover database. They should also make sure that:

- logistical material that has been exposed or compromised during deployment is recovered (for example, covert backstopping items)
- communication takes place with the appropriate host/donor undercover unit about the extent of the exposure or compromise.

Any subsequent reports which refer to the UCO (for example, commendations) should be compiled only in consultation with the undercover unit. The true identity of the UCO should not be exposed.

8.5.2 Compilation of evidence

UCOs should always have their statements typed, rather than handwritten. The operational team should have a system for compiling transcripts for subsequent checking by the relevant UCO.

The operational team makes sure transcripts are produced. Material can be outsourced to agreed secure providers for transcription.

UCOs from foreign law enforcement agencies may compile their original notes and statements of evidence in English or in the language with which they are most familiar.

8.6 Technical

Undercover operations require considerable technical support. Appropriate technical resources are accessible via the undercover unit.

When consideration is given to deploying UCOs together with technical equipment, the risk to UCOs should be balanced against operational requirements. The operational team should consider independent corroboration by other means, regardless of whether UCOs are deployed with technical equipment.

The operational lead and cover officer should agree a policy for technical equipment and recordings. This policy will be documented in the sensitive policy/decision log. Any deviation from this policy should be recorded by the cover officer as to why a technical recording has not taken place (for example, due to operational risk, technical failure or operator error).

8.6.1 Equipment

The NUWG evaluates and recommends technical equipment which is fit for purpose. In exceptional cases undercover deployments may also make use of equipment that has not been evaluated by the NUWG.

The COM-UC is responsible for making sure that UCOs and cover officers are aware of NUWG recommendations.

Where technical equipment is used, risks to the following should be considered:

- UCO
- operation
- organisation
- court process
- overall effectiveness of undercover techniques.

8.6.2 Non-NUWG evaluated equipment

The COM-UC and operational lead may decide to use equipment additional to or other than that evaluated by the NUWG. Such equipment should be approved by a technical surveillance unit.

This will be documented in the sensitive policy/decision log.

8.7 Consultation with the prosecutor

The prosecutor should be consulted in either of the following situations:

- once any material is acquired as a consequence of the use of UCOs that is capable of being presented in legal proceedings in the form of evidence (regardless of whether it is the intention of the operational lead to do so)
- at the first opportune meeting of the undercover unit and the prosecutor.

The operational lead should make sure the reviewing lawyer has enough time to consider all necessary material (evidential and unused) before being asked to provide a charging authority.

The lawyer cannot make operational decisions but they can advise on the likely evidential or disclosure implications of a proposed course of action.

The following people should be included in the consultation:

- the operational lead with primary responsibility for overseeing the UC deployment
- the senior investigating officer, where appropriate
- a member of the undercover unit.

Additional staff may be included where appropriate.

8.7.1 Example topics

Liaising with the prosecutor can deal with issues such as:

- whether the proposed parameters of the operation are likely to lead to an application to stay subsequent criminal proceedings or exclude material
- witness anonymity and special measures
- the nature of the defence case
- the extent to which any material, including authorisations, may fall to be disclosed in subsequent criminal proceedings

- the potential impact on cases not directly subject of the UCO deployment and any disclosure issues that may result.

Where UCOs are found to have instigated the commission of offences, criminal proceedings may be stayed as an abuse of process or evidence may be excluded and the operative could be liable to proceedings themselves.

9. Witness anonymity

The identity of undercover operatives (UCOs) should be protected in court proceedings.

Main points:

- there is a process for applying for witness anonymity orders, including particular paperwork
- there should be early consultation with the prosecutor, before UCOs give evidence
- COM-UCs (covert operations managers for undercover) and cover officers have responsibilities to protect UCOs giving evidence.

Contents

9.1 Witness anonymity orders

The court may provide a witness anonymity order when it is satisfied that the conditions outlined in section 88 of the Coroners and Justice Act 2009 are met. See section 89 of the Act for relevant considerations.

To comply with condition B in section 88 and with section 89, anything relevant to the UCO's credibility as a witness must be made known to the prosecutor. In all cases form MG6B (record of disciplinary findings) or equivalent must be submitted to the prosecutor for each UCO in respect of whom an order is sought.

Before an application for a witness anonymity order can be made, the COM-UC should make sure a superintendent's (or equivalent) letter of authority and an associated risk assessment are prepared and submitted to the prosecutor.

The COM-UC and cover officer should make sure there is early consultation with the prosecutor about all requests for witness anonymity orders, before any UCO gives evidence.

See also section 86 of the Act.

9.2 Letter of authority

The letter of authority should set out the protection measures that are required and explain how, in the superintendent's (or equivalent) opinion, the three conditions for making an order are met.

Section 86(2) of the Coroners and Justice Act sets out possible protection measures. These measures include screens and voice modulation.

It is often good practice to seek an order that the witness be permitted to enter and leave the courtroom in a way that does not reveal their identity.

9.3 Risk assessment

It may be appropriate for one risk assessment to be compiled for each case, which may include several UCOs.

The assessment will set out the generic and specific risks should the identity of the UCOs become known. This includes risks to the UCOs, close associations and the force or agency.

Where specific risks to UCOs are identified, the risk assessment should be retained by the relevant undercover unit and made available for consideration by the prosecutor.

9.4 Sensitive supporting documents

Where an application is supported by sensitive documents that cannot be shared with the defence, the application should be drafted in two parts.

Part one contains the material which can be served on the defence.

Part two refers to the sensitive documents which will be shown to the court but not to the defence.

9.5 Hearing of the application

The hearing of the application will be conducted in the presence of the defence. If the prosecutor needs to refer to material which comes under part two of the application, the defence will be excluded from this part of the hearing.

At no point should a statement be prepared in the true identity of UCOs.

The superintendent or equivalent or their nominated representative (usually the COM-UC) will attend court when the application is made with the original documents relied on in support of the application.

The superintendent or equivalent responsible for the undercover unit should make sure every effort is made to maintain the security of the supporting documents and the identity of UCOs during the court process.

9.6 Giving evidence

UCOs, if ordered to do so by the court, must reveal their true identity when giving evidence. This is usually done by discreetly

offering their official identification (for example, warrant card) to the judge alone.

The COM-UC and cover officer are responsible for making sure:

- there are arrangements to safely transport UCOs and keep them secure during court proceedings
- the measures outlined in the witness anonymity order are complied with.

Most courts have systems for UCOs to enter and leave the building without the risk of being identified. A change of venue can be requested via the Crown Prosecution Service where sufficient security is not available.

Security at the court should be kept under constant review while UCOs are giving evidence. Nothing should be documented or communicated to the court that could identify UCOs or their force or agency.

10. Records

Records should be kept and maintained securely to uphold the integrity of undercover operative (UCO) activity.

Main points:

- there are record keeping responsibilities which derive from legislation and policy
- records include minute sheets, sensitive policy/decision logs, deployment management records and UCO original notes
- any material that might identify a UCO should be gathered, reviewed and secured appropriately.

Contents

10.1 Record keeping

In addition to retention requirements under the Criminal Procedure and Investigations Act 1996 (CPIA), all records must be kept available for inspection by the Office of Surveillance Commissioners.

This responsibility should be managed by the senior responsible officer in the relevant organisation.

The head of unit should make sure there are processes to maintain undercover unit records and keep them secure.

Other considerations include that:

- information and intelligence should be evaluated and disseminated in accordance with the principles of information management
- records are subject to continuous review regarding their retention, inspection and dissemination
- there should be clearly defined post-deployment responsibilities, including for compiling evidence and disclosure.

10.2 Minute sheets

Each application for authorisation will be issued with a unique reference number by the central authorisations' bureau.

There should be an accompanying minute sheet that records:

- relevant dates
- whether the application is authorised, returned or refused and by whom
- all comments about the reason for a return or refusal, in addition to guidance or comments written by the authorising officer to the applicant (for example, the risk assessment requires greater detail or necessity is not clearly articulated).

Those operating an electronic system should make sure it captures and tracks all subsequent comments and amendments.

10.3 Sensitive policy/decision log

Operational leads should keep a sensitive policy/decision log. This log should include details about:

- operational objectives
- staffing
- security
- the Regulation of Investigatory Powers Act 2000
- risk assessments
- briefings and debriefings
- intelligence management
- technical
- forensic strategy
- exhibits and disclosure
- prosecutor
- media policy.

10.4 Deployment management record

UCOs may be deployed for short or protracted periods, or a combination of both. A completed deployment management record (DMR) provides:

- a unique and transparent record of the briefing and debriefing process that all those present can refer to in subsequent proceedings
- uniformity of processes
- a clear and auditable link between the operational lead's policy and the set objectives
- clear direction to UCOs on the primary requirement of case law
- a conduit for a consistent and auditable flow of intelligence.

The frequency of the briefing and debriefing process should be commensurate with the nature of the deployment. It should follow

the principles of the national briefing model and national decision model and be recorded on the DMR.

10.5 UCO original notes

UCOs should keep comprehensive records of events to an evidential standard. The undercover unit should provide UCOs with a means of recording evidence when operationally deployed (for example, an electronic or pocket notebook). These original notes should be presented regularly to the operational lead for review.

UCO original notes constitute the original record the UCO refers to in any future court proceedings. A log should be kept of the issue of all UCOs' original notes records, whether electronic or hard copy.

UCOs should record notes regarding each deployment in the respective record at the earliest opportunity. If they do not do this, they should give the reason for the delay in the original notes. The operational lead should also make a policy entry for protracted delays due to extended deployments.

10.5.1 Format and content

UCO original notes should be completed in pseudonym and any notebooks should not be readily identifiable as relating to undercover activity. Original notes should also have unique reference numbers.

When completing an entry in their original notes, UCOs should observe the 'no elbows' mnemonic (see below), as appropriate, depending on whether it is electronic or hard copy. They should include the following information:

- the time the notes started and concluded
- a detailed sequence of events
- details of exhibits, including continuity
- details of any products or conversations used to refresh their memory.

No ELBOWS mnemonic
no **E**rasures
no **L**eaves torn out
no **B**lank spaces
no **O**verwriting
no **W**riting between the lines
no **S**tatements in direct speech

10.5.2 Recordings

References to technical recordings should follow relevant guidelines. A note should be made to say that a recording was made, but the original notes should not identify the type of equipment or recording methods used. These details are kept in a separate record.

Where there has been a recording, the conversation can be paraphrased.

Where there has been no recording, a full entry of the conversation will be made. Only consider including direct speech for the salient points of the evidence.

10.6 Material that might identify a UCO

The COM-UC (covert operations manager for undercover) should liaise with the operational lead to make sure any material that might identify a UCO is gathered, reviewed and secured.

Such material could include:

- UCO original notes
- audio/visual products
- CCTV
- communications data
- surveillance products
- backstopping material.

Varying access to such material to certain groups reduces the risk of unintentionally identifying a UCO. For example, the operational team, prosecution team and defendant and defence team.

10.6.1 Operational team

In consultation with the COM-UC, specified members of the operational team will have access to original notes and associated product generated from the deployment.

Anything which could identify UCOs should be redacted before access is given. This may include redacting handwritten notes and images and audio of UCOs.

Interviewing officers should make sure no part of any covertly recorded evidence featuring UCOs is played to a suspect while the interview is being recorded. It is recommended that a transcript is provided of any appropriate conversation.

10.6.2 Prosecution team

The prosecutor must be made aware of all relevant material in line with the CPIA.

In consultation with the head of the undercover unit, the reviewing lawyer may be granted supervised access to original material.

Copies of redacted (non-technical) material may be given to the prosecution team. Assurances should be sought from the team that any material provided will be stored securely.

10.6.3 Defendant and defence team

In consultation with the prosecutor or by direction of the court, the defence team may be granted controlled access to material with appropriate safeguards. Safety measures may include redaction, pixelation and sanitisation.

When providing controlled access to material, adequate facilities should be made available so that defendants and their legal representatives can listen to recordings. Precautions should be taken to ensure the defence cannot copy or record the material.

Where defendants have been remanded in custody, recordings and recording equipment may need to be taken to the prison or remand centre. The defence may challenge these arrangements and seek a direction from the court that they are provided with copies. The operational lead should liaise with the prosecutor to

make sure all proper arguments are advanced when resisting such defence applications.

Unless ordered by a court, no video or audio product, image or other item which could identify a UCO may be served on the defence.

11. Other deployments

Some operations involve distinct challenges and should be undertaken by undercover operatives (UCOs) under specific conditions.

Main points:

- decoy operations should be undertaken by UCOs following consultations
- national security-related operations should be carried out by undercover units within counter terrorism units (CTUs)
- online operations require an undercover online operative (UCOL)
- UCOLs can be deployed at all five levels of the national internet investigation model.

Contents

11.1 Decoy operations

A decoy operation is where an operative is placed in a position where they seek to become the intended victim of a crime for the purpose of securing the arrest of the offender or gathering intelligence to further investigations.

Decoy operations are covert techniques which should, wherever possible, be undertaken by UCOs after consultation with the COM-UC (covert operations manager for undercover) and central authorisations' bureau.

Every case should be considered on its merits. Regarding authorisation of the use and conduct of a UCO, the Office of Surveillance Commissioners considers this is unlikely to be necessary in cases where there is fleeting or minimal engagement with the subject (whether or not identified).

Where an authorisation is not required, the COM-UC should retain a record of the rationale for not obtaining such an authorisation. Consideration should always be given to the requirement for other authorisations (for example, directed surveillance).

Deploying operatives in decoy operations carries a level of risk. An operational risk assessment and personal risk assessment are necessary to provide appropriate safety for the operative and show effective management and control.

11.2 National security operations

National security operations should only be undertaken by undercover units within a CTU. This is because of their unique relationship with the security services.

Where ongoing undercover operations reveal links to national security operations, the undercover unit should liaise immediately with the relevant CTU's undercover unit.

11.3 Online operations

Internet investigations cover a wide range of deployment types and are becoming more frequent in mainstream law enforcement.

Tactics employed include daily research by officers carrying out what is essentially online uniform policing, open-source research and covert network exploitation and infiltration tactics deployed by UCOs.

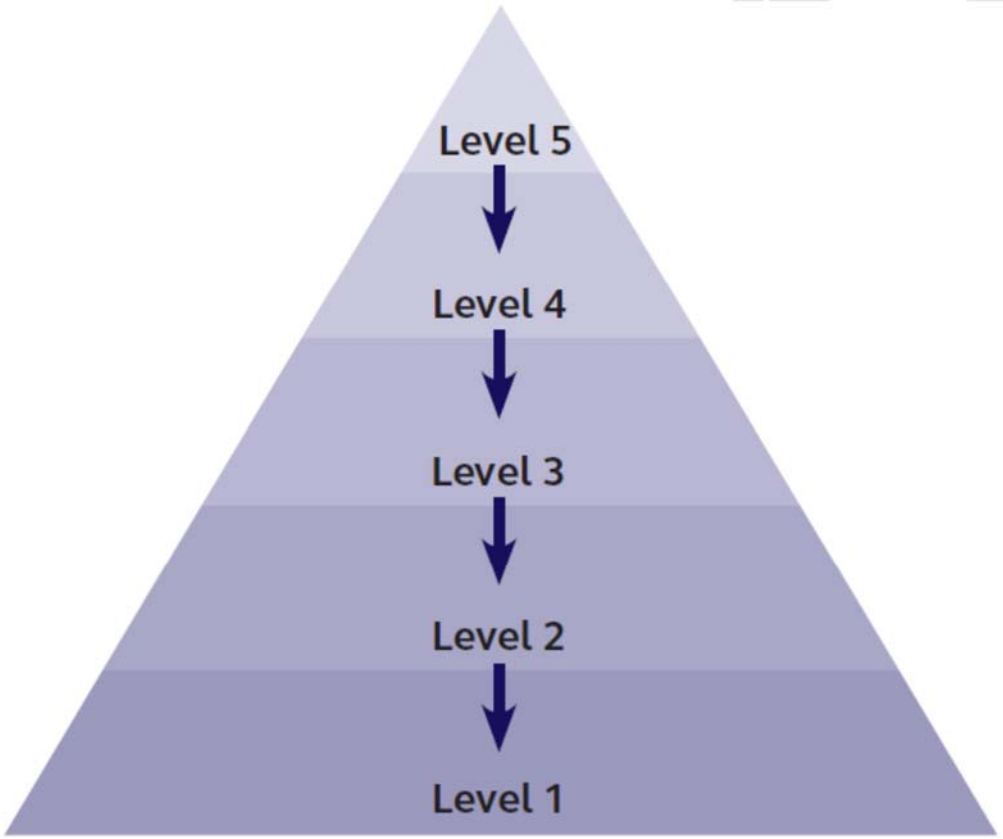
Where a relationship needs to be established or maintained via the internet, a UCOL should be deployed.

Consideration should be given to the potential psychological impact that frequently viewing graphic and disturbing images can have on UCOLs. This will be addressed and managed by an approved psychologist. See also the chapter on welfare.

11.3.1 National internet investigation model

The national internet investigation model is made up of five nationally approved levels of internet investigation/research (ACPO 2015).

UCOLs can be used in all five areas of the model.



Level 5

Online undercover operations

Level 4

Covert operations targeting subjects' internet-based accounts and footprint

Level 3

Advanced online research and surveillance

Level 2

Covert basic internet research

Level 1

Mainstream use of internet as investigative tool