

**EUROPEAN CO-OPERATION GROUP ON**  
**UNDERCOVER ACTIVITIES**

**MEMORANDUM OF UNDERSTANDING**  
**FOR THE USE OF UC OFFICERS**

Produced 17<sup>th</sup> February, 2004

**By a Sub-Group Comprising Of**

Belgium - Sven Lemmens (Chairman)

Denmark - Jan Sommer

Finland - Minna Ketola

Germany - Helmut Banschbach &  
Bernd Rossbach

Romania - Crin Cristian Popescu

United Kingdom - Carol Jenner &  
Lindsay Kearney (Secretary)

**MEMORANDUM OF UNDERSTANDING**  
**FOR THE USE OF UNDERCOVER OFFICERS**

*What are the disclosure parameters of each country that is party to this agreement in relation to this document*

*Disclosure to third parties or any other law enforcement agency must be approved by all signatories to the agreement*

(1) **APPROVAL**

Which authority approved the planned deployment or activity.

Within the approval state what is required, i.e. legend building, backstopping, training, operational deployment, etc.

Legal framework - Who is the lead agency.

What is the range of the permission.

(2) **OBJECTIVE**

The objective/purpose of the deployment/activity, for example:-

The arrest of NN, and seizure of certain goods/controlled deliveries.

Information about NN

Operating a storefront.

Facilitating on specified items i.e. training, legend building, backstopping, operational deployment, etc.

Support by an Undercover Operative.

(3) MANAGEMENT OF OPERATION/HUMAN RESOURCES

The names of the officers with operational control and their dedicated responsibilities (i.e. decision making/major discussions/disputes/costs/authority).

A good organised executive team can take away many questions so that the operative deployed can focus fully on their operational task. Disputes can be put there.

Identification details of the UC Officers i.e. operational number/pseudonym and resources deployed to be disclosed by mutual agreement. The exchange of additional information may be in a sealed envelope, verbally or by any other means.

Consideration should be given to the provision of a coverperson, i.e. will the UC be guided by his own coverperson or foreign coverperson.

(4) HARD CRITERIA

In respect of participation:-

Is the operative a trained Law Enforcement Officer, Authorised Specialist or Participating Informant, etc.

The operative must obey the law, regulations and policies of the host country as well as those of their own country.

Specify how evidence will be given in court i.e. in pseudonym, true identity, use of screens, via written report or a third person (coverperson) and security measures for personal appearances at court.

What special conditions must be obeyed, i.e. no controlled deliveries/entrapment, the committing of crime, recording of conversations, etc.

What is arranged on the carrying of firearms.

(5) COMMUNICATION

Stipulate how communication will be conducted during the deployment or activity i.e. in what language will communication take place, will it be verbal or written.

What will be the frequency of contact.

Who will be responsible for maintaining communication i.e. with the operative, with the investigative agency.

How will the activities be reported and/or documented.

(6) TIMESCALES

Consideration needs to be given to the anticipated duration of the deployment/activity and any critical deadlines that have to be met.

At what frequency will the deployment be reviewed

Who is responsible for the review process.

Determine criteria for reviewing the deployment to establish whether or not the objectives have been met.

(7) COSTS & EXPENSES

Who will meet the expenses of the deployment, i.e.

Overtime.

Accommodation.

Rental costs.

Vehicles, petrol, special equipment.

Ordinary operating expenses.

Any unanticipated expenses to be negotiated prior to expenditure.

Safehouses and storefronts (during and after the operation).

Inventory of purchased items and arrangements for the removal, distribution or disposal of them.

It may be advantageous to review the financial aspects of the deployment on a regular basis.

When are payments for expenses to be made, i.e. before the deployment, afterwards or at regular intervals.

Are there special rules/appointments necessary for taxes (income taxes/storefront activities taxes).

In the event of a compromise to an operative or informant consideration should be given to who would support the possible protection programme costs.

Consideration to be given to the division of any income derived from the deployment, seized/confiscated assets.

(8) INSURANCES

The insurance arrangements for a deployment should be determined, i.e. for the Law Enforcement Officer, Authorised Specialist or Participating Informant, etc.

Are resources adequately insured, i.e. storefronts, furniture, vehicles, etc.

(9) DISCLOSURE

Disclosure to third parties or any other law enforcement agency must be approved by all signatories to the agreement

A media policy should be agreed by all parties.

(10) SAFETY

Who is responsible for conducting the risk assessment. (A sample risk assessment is attached at Appendix 'A').

What are the possible risks that are expected and how will be anticipated on the safety of the employees involved. (Technical and tactical surveillance, intervention/arrest team, etc., - provided by whom?)

(11) BRIEFING & DE-BRIEFING

Who is responsible within the organisation for arranging briefings and de-briefings.

What are the parameters and the frequency of briefings and de-briefings.

Consideration should be given to briefing and de-briefing of non-operational deployments, i.e. legend building to be conducted with the host country for the benefit of all concerned.

(12) OTHER CONSIDERATIONS

Are there any other considerations to be taken account of?

SIGNATURE PARAGRAPH OF COMPETENT AUTHORITIES

The responsible authorities must sign the Memorandum of Understanding.

17<sup>th</sup> February, 2004.

U.K. RISK ASSESSMENT CONSIDERATIONS

**1. Risk Assessment for CHIS and/or UCO(s).**

A risk assessment must be completed in respect of each application and must be reassessed when each application is reviewed/renewed.

Comment on the actual or apparent risk using the PPPLEM risk assessment module.

Consider the following: (This is not an exhaustive list)

**POLICE and community concerns:**

- Can the protection of sensitive policing techniques be adequately managed?
- Comment on any adverse impact on community confidence or safety that may result from the proposed activity in the event of a compromise?
- Is there a risk of disproportionate damage to our professional reputation if the operation is exposed, equipment compromised or a prosecution collapses?

**PHYSICAL risks to CHIS/UCO (and Operational Team supporting):**

- Do the CHIS and/or UCO(s) and members of public who may assist or be subjected to collateral intrusion face any physical risks?
- Are there any risks to the safety of the subject(s)?
- What support measures are in place?
- What exposure has the CHIS had to covert methods?
- Where there are no significant risks to the CHIS and/or UCO(s) consider any risks to the operation by the use of the CHIS and/or UCO(s).

**PSYCHOLOGICAL pressure apparent on CHIS/UCO (and Operational Team supporting):**

- Consider the psychological pressures that may be experienced by CHIS and/or UCO(s), placed in vulnerable positions.
- Are the CHIS and/or UCO(s) comfortable with the task(s) requested of them?
- Are the UCO(s) sufficiently competent to carry out the task in terms of knowledge, training and experience?

**LEGAL issues involved in the use of the CHIS/UCO:**

- Are CHIS and/or UCO(s) conversant with their responsibilities and case law?
- Are legal guidelines/instructions being adhered to and is there a high level of legal or media interest in the case?
- Have Public Interest Immunity (PII) issues been considered?
- Early consultation with CPS, where appropriate, must be considered.
- Can the authorised participation be justified if it became known to the public?
- Keep the possibility of participation and agent provocateur prominent in our assessment?

**ECONOMIC considerations (potential impact of compromise):**

- Consider the possible cost implications in the light of a compromise (e.g. witness protection)
- Does the use of a CHIS and/or UCO(s) provide the means of obtaining information/intelligence/evidence thereby reducing the need to deploy other more costly methods?

**MORAL and ethical issues raised by the use of CHIS/UCO.**

- Is it morally justified to deploy the CHIS and/or UCO(s)?
- Has an exit strategy for CHIS been discussed and agreed?
- Does the CHIS present any moral threat to particular communities or groups?