Sunderland City Council

Guidance to Staff

on the

Regulation of Investigatory

Powers Act 2000

Directed Surveillance and Use of Covert

Human Intelligence Sources

INDEX

PROCEDURE SUMMARY 2019

Directed Surveillance activities undertaken by, or on behalf of, the Council must be authorised by the relevant senior officers below. The same applies where the Council proposes to make use of a covert human intelligence source. Authorised applications must then be approved by a Magistrate before the activity becomes lawful under RIPA. (see section 5.1.1.3)

The Central Register of Authorisations is held by the RIPA Coordinating Officer (RCO) (see Section 5).

Where time allows, a draft of every authorisation, review, renewal and cancellation should be provided to the RCO, for review and comment, before authorisation is granted.

Every authorisation, review, renewal and cancellation made must be forwarded promptly to the RCO for inclusion on the Central Register. (see Section 5 Authorisations, Renewals and Duration).

Authorising and Investigating Officers are required to identify and log **all** surveillance equipment deployed and / or used in the completion of a given directed surveillance activity. A record of equipment deployed and / or used should be kept in the investigation file in question and a copy passed to the DPO for addition to the RIPA Central Register.

Forms for authorisation, review, renewal and cancellation are available at Appendix 3 (LINK to forms) and are to be used in the place of previous forms. No use is to be made of outdated forms previously issued, and any remaining stock of these is to be destroyed.

RELEVANT SENIOR OFFICERS

SENIOR RESPONSIBLE OFFICER (SRO)

Name	Job Title	Directorate

AUTHORISING OFFICERS (AO)

Name	Job Title	Directorate

RIPA COORDINATING OFFICER (RCO)

Name	Job Title	Directorate

NB:

- Only the Chief Executive or, in his absence, the person acting as Head of Paid Service, can authorise use of a juvenile source.
- Only the Chief Executive or, in his absence, the person acting as Head of Paid Service, have the power to authorise directed surveillance, which involves the covert filming of any officer.
- This list is to be maintained and notification of any change of relevant personnel given to the RCO to allow the list to be updated within 7 days.

1. Introduction

1.1 This Guidance addresses the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) which regulates any covert investigations carried out by a number of public bodies, including local authorities, and its codes of practice. The Act was introduced to ensure that individuals' human rights are protected while also ensuring that the UK's law enforcement and security agencies have the powers they need to do their job effectively. It applies in relation to the covert surveillance of individuals, including recording, and the use of covert human intelligence sources, including undercover officers, agents and informants.

1.2 This guidance support's the Council's commitment to work within the RIPA framework with regard to the authorisation of both Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS), to carry out investigations in a fair and equitable manner that respects the human rights of individuals.

1.3 The purpose of this guidance is to;

- Explain the scope of RIPA and the circumstances where it applies
- Provide guidance on the procedures to be followed in respect of authorisations, renewals and cancellations.

1.4 The overt use of CCTV systems is covered by a separate Council policy statement and code of practice.

1.5 This guidance provides officers with an overview of their responsibilities. It is not a comprehensive statement of the requirements that must be observed and all officers involved in directed surveillance or CHIS activity must familiarise themselves with the detailed guidance provided in the relevant Codes of Conduct and obtain advice as appropriate. Any service using covert operations is expected to comply with the authorisation procedures in accordance with the legislation and the Codes of Practice produced by the Home Office. This guidance gives an overview only of those aspects of RIPA most pertinent to the council's operations. Officers considering the use of technologies, including recording telephone calls and use of emerging technologies such as drones for aerial surveillance, should consult the relevant sections of the codes of practice and always seek advice on whether authorisation is required.

The Codes of Practice are available online at;
https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice.

1.6 The Act requires that when the Council undertakes "directed surveillance" or uses a "Covert Human Intelligence Source" ("a source") these activities are authorised by an officer with delegated powers, and only when the relevant criteria are satisfied. The list of Authorising Officers is at page 3.

1.7 Authorisation under RIPA gives lawful authority to carry out surveillance and the use of a source. Obtaining authorisation helps to protect the Council and its officers from complaints of interference with the rights protected by Article 8 (1) of the European Convention on Human Rights which is enshrined in English law through the Human Rights Act 1998. This is because the interference with the private life of citizens will be "in accordance with the law". Provided the activities undertaken are also "reasonable and proportionate" they will not be in contravention of Human Rights legislation.

1.9 The Council can only authorise covert activity under RIPA for the purpose of an investigation that is necessary for the purpose of preventing or detecting crime that is punishable by a maximum tariff of at least 6 months imprisonment, or that is related to the underage sale of alcohol, tobacco or nicotine inhaling products.

1.10 The Council cannot authorise "Intrusive Surveillance". Intrusive Surveillance is described at paragraph 2.3 to 2.5 inclusive.

1.11 Neither can the Council or any Council Officer authorise entry on property.

1.12 Deciding when authorisation is required involves making a judgment. The Codes of Practice provide useful examples that should be referred to. For example, where intelligence suggests that underage sales of alcohol are taking place and trading standards officer might then visit the shop in question and made a test purchase as part of their enforcement functions. Where this does not involve the forming of a relationship with the shopkeeper or another person, and does not involve the systematic surveillance of an individual, it forms a part of the everyday functions of law enforcement or other public bodies and will not usually be regulated under RIPA. Conversely where systematic covert surveillance is undertaken then an authorisation will be required.

Where, for example, investigators knock on a suspect's door to ascertain whether they do in fact live at that address, then provided they identify themselves and the purpose of the call no authorisation is required since the approach is overt and not covert.

Neither do the requirements of RIPA or this guidance cover the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime, and the systems are clearly signposted. Covert use of CCTV as part of a planned operation, however, will require authorisation.

If you are in doubt, seek the advice of an Authorising Officer. If they are in doubt they should contact the RIPA Coordinating Officer to seek specialist advice

1.13 Only the Head of Paid Service or, in his absence, the person acting as Head of Paid Service, can authorise use of a juvenile source.

Only the Chief Executive and Assistant Director of Law & Governance have the power to authorise directed surveillance, which involves the covert filming of any officer.

1.14 The RCO will maintain a Central Record of all authorisations for covert surveillance, reviews, renewals and cancellations, and monitor them to ensure uniformity of practice. The SRO will also examine the Central Record on a routine basis, to ensure compliance.

1.14 Each Directorate is to retain its authorisations, reviews, renewals and cancellations on a secured and controlled centralised file, and ensure a copy is put on the individual case file,
The Authorising Officer will, within 7 days of authorisation, forward a further copy to the RCO for the Central Record, in a sealed envelope marked "confidential". Authorising Officers will ensure that a copy of each authorisation, renewal and cancellation is forwarded promptly.

1.15 Roles and Responsibilities

1.15.1 Senior Responsible Officer (SRO)

The SRO is available to advise on procedure and is responsible for:

- the integrity of the process in place within the Council to authorise directed and intrusive surveillance and interference with property or wireless telegraphy and for the management of CHIS;
- compliance with Part II of the 2000 Act, Part III of the 1997 Act, section 5 of the 1994 Act and with the Codes of Practice;
- Oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the Investigatory Powers Commissioner and inspectors who support the Commissioner when they conduct their inspections;
- overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner, and;
- Ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

1.15.2 Authorising Officers (AO)

The role of the Authorising Officers is to authorise, review, renew and cancel directed surveillance.

Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved. Where an Authorising Officer authorises such an investigation or operation the Central Record of Authorisations should highlight this, and it should be brought to the attention of a Commissioner or Inspector during their next inspection.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for local authorities the Authorising Officer shall be a Director, Assistant Director, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation.

A designated Authorising Officer must qualify both by rank and by competence. Officers who wish to be designated must have been trained to an appropriate level so as to have an understanding of the Act and the requirements that must be satisfied before an authorisation can be granted.

Authorisations must be given in writing by the Authorising Officer. They must complete the relevant section on the application form. The Authorising Officer must believe the surveillance is proportionate to what it seeks to achieve, taking into account the collateral intrusion issues, and that the level of the surveillance is appropriate to achieve the objectives.

If any equipment such as covert cameras, video cameras is to be used, the Authorising Officer should know the capability of the equipment before Authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. They should not rubber-stamp a request. It is important that they consider all the facts to justify their decision. They may be required to justify their actions in a court of law or some other tribunal.

Authorising Officers are also responsible for carrying out regular reviews of applications which they have authorised and also for the cancellation of authorisations.

Authorised Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and guidance provided by the Investigatory Powers Commissioner (IPC).

1.15.3 Investigating Officers (IO)

Investigating Officers should consider carefully whether there is a need to undertake DS or CHIS before they seek authorisation. Investigating Officers need first to consider whether they can obtain the information by using techniques other than covert surveillance. There is nothing that prevents an Investigating Officer discussing the issue of surveillance beforehand.

IOs should then discuss investigative requirements with line managers, Authorising Officers and / or Legal Services (as necessary) to determine whether RIPA authorisation is a necessary step to take in pursuing the investigation.

1.15.4 RIPA Co-Ordinating Officer (RCO)

The RIPA Co-Ordinating Officer will coordinate advice and guidance on RIPA issues and maintain the Council's Central Register of Authorisations in accordance with relevant guidance and the Codes of Conduct.

2. Directed Surveillance

NOTE: you must seek RIPA authorisation before undertaking "directed surveillance"

2.1 What is meant by Surveillance?

"Surveillance" includes;

a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;

b) recording anything monitored, observed or listened to in the course of surveillance; and

c) surveillance by or with the assistance of a surveillance device.

For RIPA purposes surveillance does not include:

a) any conduct of a covert human intelligence source for obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source; (for example, if you confront a neighbour with evidence obtained by a professional witness tenant in an attempt to shame them into better behaviour).

b) the use of a covert human intelligence source for so obtaining or recording information, or any entry on or interference with property or wireless telegraphy as would be unlawful unless authorised under warrants for the intelligence service legislation or powers of police and customs officers.

2.2 When is surveillance directed?

Surveillance is 'Directed' if it is covert, but not intrusive and is undertaken:

a) for the purposes of a specific investigation or a specific operation.

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not this is specifically identified for the purposes of the investigation or operation); and

c) is carried out for reasons other than an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

2.3 **When is surveillance intrusive?**

NOTE: The Council is not authorised to carry out intrusive surveillance. Surveillance becomes intrusive if the covert surveillance is:

a) carried out in relation to anything taking place on any "residential premises" or in any "private vehicle"; and

b) involves the presence of an individual or surveillance device on the premises or in the vehicle or is carried out by means of a surveillance device; or

c) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

If the device is not on the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as if it were.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

Surveillance relating to legal consultations and/or carried out in courts, police stations or legal adviser's offices is also considered intrusive.

2.4 **Does RIPA apply?**

Before any officer of the Council undertakes any surveillance of any individual or individuals they need to assess whether the activity comes within the 2000 Act. In order to do this the following key questions need to be asked.

2.4.1 **Is the surveillance covert?**

Surveillance is covert if it is carried out in a manner (calculated) to ensure that subjects of it are unaware it is or may be taking place.

If activities are open and not hidden from the subjects of an investigation, the 2000 Act framework does not apply. This includes the overt use of CCTV and ANPR systems.

2.4.2 **Is it for the purposes of a specific investigation or a specific operation?**

For example, are Town Centre CCTV cameras which are readily visible to anyone walking down the street covered?

The answer is; not if their usage is to monitor the general activities of what is happening in the street. However, if that usage changes, the 2000 Act may apply.

For example, if the CCTV cameras are targeting a particular known offender, and we have been asked to assist law enforcement agencies in tracking his activities, that has turned into a directed surveillance operation, and will require authorisation.

2.4.3 **Is it in such a manner that it is likely to result in the obtaining of private information about a person?**

"Private Information" is any information relating to a person's private or family life. As a result private information may include any aspect of a person's private or personal relationship with others, such as family and professional or business relationships. By contrast, information that is publicly available, for example through books, newspapers, TV, websites, business publications etc is not considered private.

For example, if part of an investigation is to observe an individual's home to determine their comings and goings then that would be covered. Private information is not, however, confined to information within the home. The law in this area is developing and the definition may include information gathered from observations made in a public, work or professional setting. Advice should be sought when considering surveillance that may impact on an individual in a situation where they may have an expectation of privacy, for example in a situation where a member of the public may have a reasonable expectation of privacy when in conversation on the street or on a bus, or where a member of staff may have a reasonable expectation of privacy within the workplace.

If it is likely that observations will not result in the obtaining of private information about a person, then it is outside the RIPA framework.

2.4.4 **What if we need to act immediately?**

You need to obtain authorisation for surveillance in every case with the exception of circumstances where it is a necessary immediate response to an event or circumstances where it is not reasonably practicable to get authorisation.

This is applicable where action is taken as an immediate response to something happening during the course of an observer's work which is unforeseeable.

However, if as a result of an immediate response, a specific investigation subsequently takes place that brings it within the 2000 Act framework.

3. Covert use of Human Intelligence Source (CHIS – also known as a "source")

3.1 A person is a source if:

a) s/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) s/he covertly uses such a relationship to obtain information or provide access to any information to another person; or

c) s/he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

3.2 A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose; and

3.3 This clearly covers the use of professional witnesses to obtain information and evidence. For example, it will include professional witnesses retained to obtain information and evidence against alleged nuisance perpetrators.

It may also cover "entrapment cases" if the foregoing criteria were established. For example, Licensing Officers or Police Officers who at their instigation pretend to be fares to catch the unwary private hire vehicle doing unlicensed pick-ups, but only if, in doing so, they develop a degree of relationship with the driver, that goes beyond the mere transaction.

An officer entering a shop and making a test purchase does not require an authorisation, unless a degree of relationship is built up with the shopkeeper, for example where a number of visits are made without the officer identifying him/herself as an investigator. However, where the test purchase is to be made by another person (for example a juvenile, where the investigation is directed at establishing whether the shopkeeper observes the law regarding under age sales) then the covert attendance of an officer to observe the transaction does require authorisation, if it fulfils the criteria for directed surveillance.

3.4 Officers should be particularly alert to the potential for a CHIS relationship to arise where, for example, they receive information from a member of the public who is asked, or who indicates, they intend to continue to monitor a

situation e.g. through the covert manipulation of an existing relationship. CHIS relationship arises at the point the relationship is formed or maintained in order to supply information. This includes situations where the officer does not request ongoing covert activity but envisages it may take place unrequested.

If in doubt officers should seek authorisation.

4. Social Media and the Internet

Any officer considering internet / social media investigation of individuals must first consider the detailed guidance provided in the codes of practice and consult with their service manager and the RIPA Co-ordinating Officer.

4.1 The Internet can be a powerful tool supporting Council investigations – websites and social media allow ready access to information. As a public body, the Council needs to balance the power of the internet with our obligations to remain within the law.

4.2 Basic Principles

While it is possible to obtain significant information about individuals without leaving the office, the same principles apply as would in the case of information we might gather by following, photographing or filming individuals. Officers should view the internet in the same way as they would view information received directly from a complainant, a witness or a suspect in 'the real world'.

4.2.1 Initial Google Searches

A Google search for an individual may be thought of as an initial 'drive-by' observation in an investigation. It is broadly equivalent to an officer responding to an initial complaint or tip-off and visiting a particular location to establish 'the lay of the land'. It doesn't gather significant, detailed or private information, but it is a starting point that allows us to decide if more detailed and directed investigation is required and / or possible.

An initial Google (or similar) search is not covert or directed surveillance and is unlikely to require RIPA authorisation.

Details of any such searches and their results should, however, be recorded in any notes or records of a given case.

4.2.2 Detailed Google Searches

While initial Google search results are equivalent to an initial drive-by in a case, if this is continued covertly and becomes a focussed search, likely to result in the obtaining of private information about a person or group the activity becomes 'directed' within the definition of Directed Surveillance.

A shift into the definition of Directed Surveillance is significantly more likely when an initial google search produces social media links for a person under investigation.

4.2.3 Social Media information

An initial look on social media platforms such as Facebook, LinkedIn, Twitter and others can usually be viewed in the same way as an initial google search: that is, an officer is looking to see if a particular person has an online presence– the officer is simply looking to see if there are any resources that might provide lines of enquiry in future, more detailed, investigation.

However, returning to look at / into a person's online presence in more detail in order to monitor it or extract information relevant to an investigation is likely to require authorisation and advice must be taken on whether authorisation is required before proceeding.

Anyone cultivating an online relationship with an investigation subject (for example, a 'friend request' or similar) is likely to be moving into the scope of CHIS investigations, and advice must be taken on whether authorisation is required before proceeding.

5 Authorisations, renewals and duration

5.1 The Conditions for Authorisation

5.1.1 Directed Surveillance

5.1.1.1 For directed surveillance no Council officer shall grant an authorisation for the carrying out of directed surveillance unless s/he believes:

a) that an authorisation is necessary for the purpose of preventing or detecting crime or of preventing disorder; and

b) the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

Note that proportionality requires –

i) that the proposed covert surveillance is proportional to the mischief under investigation
ii) that it is proportional to degree of anticipated intrusion on the target and others, and
iii) it is the only option – other overt means having been considered and (reasonably) discounted.

5.1.1.2 The onus is therefore on the person authorising such surveillance to satisfy themselves it is:

a) necessary; i.e. that all other available options have been weighed up and found to be unsatisfactory. Factors to consider include consideration of the aims and objectives of the surveillance exercise (which must be for the purpose of preventing and detecting crime or of preventing disorder), whether there are alternative courses of action, or enquiry, whether the information to be obtained is likely to significantly benefit the enquiry or chance of prosecution. Authorising officers must remind themselves that surveillance is an intrusion into a person's privacy and should only be considered as a last resort.

b) is proportionate to its aim; Authorising Officers must evaluate the size and scope of an application against the gravity and extent of the perceived mischief; they must be satisfied that methods proposed will cause the least possible intrusion on a target or others; they must be satisfied that any operation is an appropriate use of RIPA provisions in preference to other available options. If in doubt as to the proportionality of the proposed surveillance Authorising Officers must contact the RCO to seek advice.

In order to ensure that authorising officers have sufficient information in order to make an informed decision it is important that detailed records are maintained using the forms in the Appendix 3. Detailed information should be given in applications regarding necessity and proportionality, sufficient for an authorising officer to make an informed decision. When completing the forms officers should try to cover the principles thoroughly but without repeating information unnecessarily.

When completing an application, the case must be presented in a fair and balanced way and present any relevant information that weakens the case for a grant of authorisation.

The authorising officer must take account of the risks of collateral intrusion and identify the measures to be taken to mitigate these, if it is considered proportionate to proceed.

An authorisation must be wide enough to cover all the measures required, but no wider than is necessary to achieve the objectives of the surveillance. This will permit effective monitoring of what is done against what is authorised.

5.1.1.3 Authorising Officers must obtain Magistrates' approval of the authorisation before the activity can proceed. Home Office Guidance on the Magistrates' Approval Process is provided at Appendix 2(e), the brief process being as follows -

a) The first stage will be to apply for an internal authorisation in the usual way. Once it has been granted, the local authority will need to contact the local Magistrates Court to arrange a hearing.

b) The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP. It is envisaged that the investigating officer will be best suited to fulfill this role. The local authority may consider it appropriate for the SPoC (Single Point of Contact) to attend for applications involving communications data.

c) The local authority will provide the JP with a copy of the original RIPA authorisation or notice. This forms the basis of the application to the JP and should contain all information that is relied upon. In addition, the local authority will provide the JP with two copies of a partially completed judicial application/order form (which is included in the Home Office Guidance).

d) The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters. The forms and supporting papers must provide sufficient information by themselves to make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided.

e) The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. He/She will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met (see below).

f) The order section of the above-mentioned form will be completed by the JP and will be the official record of the his/her decision. The local authority will need to retain a copy of the form after it has been signed by the JP.

The JP may decide to –

- *Approve the grant or renewal of an authorisation or notice*

The grant or renewal of the RIPA authorisation or notice will then take effect and the local authority may proceed to use the technique in that particular case. The local authority will need to provide a copy of the order to the

communications service provider (CSP), via the SPoC (Single Point of Contact), for all CD requests.

- *Refuse to approve the grant or renewal of an authorisation or notice*

The RIPA authorisation or notice will not take effect and the local authority may not use the technique in that case. Where an application has been refused the local authority may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the local authority going through the internal authorisation process again. The local authority may then wish to reapply for judicial approval once those steps have been taken.

- *Refuse to approve the grant or renewal and quash the authorisation or notice*

This applies where a Magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice.The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least two business days from the date of the refusal in which to make representations.

Appeals

A local authority may only appeal a JP's decision on a point of law by making an application for judicial review in the High Court. The Investigatory Powers Tribunal (IPT) will continue to investigate complaints by individuals about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT finds fault with a RIPA authorisation or notice it has the power to quash the JP's order which approved the grant or renewal of the authorisation or notice. It can also award damages if it believes that an individual's human rights have been violated by the public authority doing the surveillance.

5.1.1.4 Investigating and Authorising Officers must record any **surveillance equipment** deployed and / or used in pursuit of a given authorisation using the form at Appendix 3(f)

5.2 Covert Use of Human Intelligence Sources

5.2.1 The same principles of necessity and proportionality apply, as with Directed Surveillance (see paragraph 5.1.1.2 above).

5.2.2 The conduct so authorised is any conduct that:

a) is comprised in any such activities involving conduct of a covert human intelligence source, or the use of a covert human intelligence source, as are specified or described in the authorisation.

b) consists in conduct by or in relation to the person who is so specified or described as the person to whose actions as a covert human intelligence source the authorisation relates; and

c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

5.2.3 In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. The forms in the Appendices must be completed and the requirements of the Source Records Regulations addressed (see Appendix 2). Detailed information should be given in applications regarding necessity and proportionality, sufficient for an authorising officer to make an informed decision regarding the tests set out at para 5.1.1.2.

An authorisation must be wide enough to cover all the measures required, but no wider than is necessary to achieve the objectives of the surveillance. This will permit effective monitoring of what is done against what is authorised.

All authorisations MUST include the appointment of a Controller and Handler to manage the CHIS operation, keep appropriate records and ensure the safety of the Source, in accordance with the Home Office Code of Practice on Covert Human Intelligence Sources. Controller and Handler must be adequately trained in CHIS management and handling, and cannot be the same officer.

5.2.4 Although it is possible to combine two authorisations in one form the Council's practice is for separate forms to be completed to maintain the distinction between Directed Surveillance and the use of a source.

5.2.5 The Code of Practice makes it clear that the 2000 Act can interfere with Article 8 of the Human Rights Act 1998, where information about the private or family life of another person is obtained covertly.

5.2.6 There is no geographical limit on a source – authorisations can be obtained both in and out of the UK.

5.2.7 Nothing in the 2000 Act prevents material obtained from the use or conduct of the source being used in evidence in Court proceedings. Existing Court discretion and procedures can protect, where appropriate, the disclosure of the source's identity.

5.2.8 The Authorising Officer, Controller and Handler must consider the safety and welfare of that source, and the foreseeable consequences to others of

the tasks they are asked to carry out. A risk assessment should be carried out before authorisation is given. Consideration of the safety and welfare of the source, even after cancellation of the authorisation, should also be considered.

5.2.9 In accordance with the Source Records Regulations, accurate and proper recording keeping should be kept about the source and tasks undertaken although the confidentiality of the source must be maintained.

5.2.10 The Authorising Officer must ensure that satisfactory arrangements exist for the management of the source in accordance with paragraph 4.2.3 above.

5.2.11 A source may, in the context of an authorised operation, infiltrate existing criminal activity, or be a party to the commission of criminal offences, within the limits recognised by law. A source who acts beyond these limits will be at risk of prosecution. The need to protect the source cannot alter this principle.

5.2.12 Before authorising the use or conduct of a source, the authorising officer should believe that the conduct/use including the likely degree of intrusion into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. He should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

5.2.13 Particular care should be taken in circumstances where people would expect a high degree of privacy or where, as a consequence of the authorisation, “confidential material” is likely to be obtained.

5.2.14 Consideration should also be given to any adverse impact on community confidence that may result from the use or conduct of a source or information obtained from that source.

5.2.15 Additionally, the Authorising Officer should make an assessment of any risk to a source in carrying out the conduct in the proposed authorisation.

5.2.16 **Cultivation of a source**

Cultivation is the process of developing a relationship with a potential source, with the intention of:

- Covertly making a judgement as to his/her likely value as a source of information;
- Covertly determining whether and, if so, the best way in which to propose to the subject that he/she become a source.

5.2.17 It may be necessary to infringe the personal privacy of the potential source in the process of cultivation. In such cases, authorisation is needed for the

cultivation process itself, as constituting the conduct (by the person undertaking the cultivation) of a source.

5.2.18 **Use and conduct of a source**

Authorisation for the use and conduct of a source is required prior to any tasking. Tasking is an assignment given to the source, asking him or her to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. It may involve the source infiltrating existing criminal activity in order to obtain that information. It may include the source using an internet profile to establish or maintain a relationship.

5.2.19 **Vulnerable individuals**

Vulnerable individuals, such as the mentally impaired, may only be authorised to act as source by the Head of Paid Service and in the most exceptional circumstances.

5.2.20 **Juvenile sources**

Special safeguards also apply to the authorisation for the use or conduct of juvenile sources; that is sources under the age of 18 years. Only the Head of Paid Service, or, in his absence, the person acting as Head of Paid Service may authorise the use of a juvenile source. On no occasion should the use or conduct of a source under 16 years of age to give information against his or her parents be authorised. In other cases, authorisations should not be granted unless:

- A risk assessment has been undertaken as part of the application to deploy a juvenile source, covering the physical dangers and the psychological aspects of his or her deployment;

- The risk assessment has been considered by the authorising officer and he has satisfied himself that any risks identified in it have been properly explained; and

- The Authorising Officer has given particular consideration as to whether the juvenile is to be asked to get information from a relative, guardian or any other person who has for the time being assumed responsibility for his welfare.

As stated at 3.2 a juvenile making a test purchase will not be a CHIS in circumstances where no relationship is formed with the seller.

5.2.21 In addition juvenile authorisations should not be granted unless the Authorising Officer believes that arrangements exist which will ensure that there will at all times be a person who has responsibility for ensuring that an appropriate adult will be present between any meetings between the authority and a source under 16 years of age.

5.3 **Summary of Factors to Consider**

5.3.1 Any person giving an authorisation should first satisfy him/herself that the authorisation is necessary on particular grounds and that the surveillance is proportionate to what it seeks to achieve. Authorising officers should specify in their own words what they are authorising. They must direct their mind to the circumstances of the individual case. Authorising officers must record the time of the commencement of the authorisation.

5.3.2 Particular consideration should be given to collateral intrusion on or interference with the privacy of persons other than the subject(s) of surveillance.

5.3.3 An application of an authorisation should include an assessment of the risk of any collateral intrusion or interference. This will be taken into account by the authorising officer, particularly when considering the proportionality of the surveillance.

5.3.4 Those carrying out the covert surveillance should inform the authorising officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

5.3.5 Any person giving an authorisation will also need to be aware of any particular sensitivities in the local community where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

5.3.6 The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance near his/her home, or where there are special sensitivities.

5.3.7 **Seal of Confession**

No operations will be undertaken in circumstances covered by the Seal of the Confession. In addition, where they are satisfied that a Minister of Religion is not him/herself involved in the matter under investigation, and they believe that surveillance will lead to them intruding on spiritual counselling between the Minister and a member of his/her faith, they should, in preparing the case for authorisation, given serious consideration to discussing the matter first with a relevant senior representative of the religious authority. The views of the senior representative would be included in the request for authorisation. In this respect, spiritual counselling is defined as conversations with a Minister of Religion acting in his/her official capacity which does not amount to a sacramental confession, but where the person being counselled is seeking or the

Minister is imparting forgiveness, or absolution of conscience with the authority of the Divine Being of their faith.

5.3.8 **Confidential Material**

RIPA does not provide any special protection for 'confidential material' (see the definitions in Appendix 1). Nevertheless, such material is particularly sensitive, and is subject to additional safeguards under the Home Office code. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the source should be subject to special authorisation by a Chief Officer or Deputy Chief Officer.

5.3.9 In general, any application for an authorisation which is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

5.3.10 The following general principles apply to confidential material acquired under Part II authorisations: -

- Those handling material from such operations should be alert to anything which may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from a legal adviser before further dissemination takes place;

- Confidential material should not be retained or copied unless it is necessary for a specified purpose;

- Confidential material should be disseminated only where an appropriate officer (having sought advice from a legal adviser) is satisfied that it is necessary for a specific purpose;

- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.

- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

5.3.11 Combined authorisations

In cases of joint working i.e. with other agencies on the same operation, authority for directed surveillance by the Housing Benefit Investigator must be obtained from the LA authorising officers. Authority cannot be granted by Benefits Agency authorising officers for the actions of LA staff and vice versa.

5.3.12 Although it is possible to combine two authorisations in one form the Council's practice is for separate forms to be completed to maintain the distinction between Directed Surveillance and the use of a source.

5.4 Review

5.4.1 Authorising Officers should ensure regular review of each authorisation. Reviews should take place at an interval of no more than 28 days, or earlier in the case of surveillance operation involving particularly sensitive issues, such as the obtaining of confidential information, or high risk of collateral intrusion. Where a surveillance operation is anticipated to be of shorter duration, arrangements should be made for earlier review. On each review the Authorising Officer shall consider whether the authorisation should remain in place. (See 4.3.8 to identify AO in cases involving confidential information)

5.4.2 The review should also include consideration of; developments since the authorisation was given, the number of days on which surveillance has been carried out, whether the surveillance has achieved its objectives, whether amendments are required to the authorisation.

5.4.3 Authorising Officers reviewing an authorisation which is not to be cancelled shall ensure the record is updated appropriately.

5.6 Renewals

5.6.1 Authorisations lapse, if not renewed:

- within 72 hours if either granted or renewed orally, (or by a person whose authorisation was confined to urgent cases) beginning with the time of the last grant or renewal, or
- 4 months, if it is for the conduct or use of a juvenile as a covert human intelligence source, or
- 12 months – if in writing/non-urgent – from date of last renewal if it is for the conduct or use of a covert human intelligence source or
- in all other cases (i.e. directed surveillance) 3 months from the date of their grant or latest renewal

5.6.2 An authorisation can be renewed at any time before it ceases to have effect by any person entitled to grant a new authorisation in the same terms.

However, for the conduct of a covert human intelligence source, a person should not renew unless a review has been carried out and that person has

considered the results of the review when deciding to renew or not. A review must cover what use has been made of the source, the tasks given to them and information obtained.

5.7 Handling and disclosure of product

5.7.1 Authorising officers are reminded of the guidance relating to the retention and destruction of confidential material as described in paragraph 4.3.10 above.

5.7.2 Authorising officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after directed surveillance activity is no longer necessary.

5.7.3 Authorised officers must ensure that copies of each authorisation are sent to the IGT as described in paragraph 5 below.

5.7.4 Applications for directed surveillance are to be securely retained by the authorising officer, for a period of 5 years. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review. Once the investigation is closed (bearing in mind cases may be lodged sometime after the initial work) the records held (save of course for the copy of the Authorisation itself) by the Department should be disposed of in an appropriate manner (e.g. shredded).

5.7.5 Authorising officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the authorising officer. Where enforcement action is likely to follow, the officer must ensure that all material associated with the investigation is retained to be made available for disclosure to the Defence as unused material when proceedings have been initiated.

Similarly if there is reason to believe that material obtained during the course of an investigation might be relevant to another investigation or to any pending or future civil or criminal proceedings, then it must not be destroyed but should be retained as it will form part of the unused prosecution material.

5.7.6 There is nothing in the 2000 Act that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the authority which authorised the surveillance, or the courts, of any material obtained by means of covert surveillance and, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances.

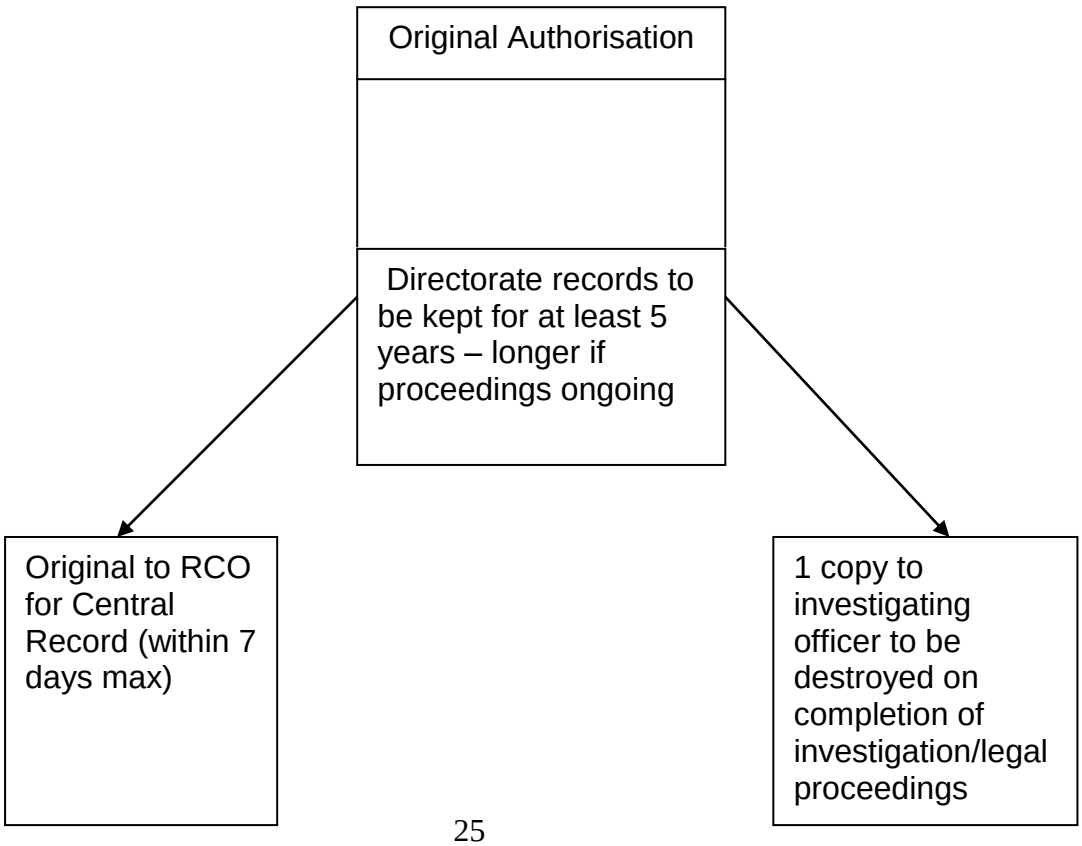
6. Central Register of Authorisations

6.1 The 2000 Act requires a central register of all authorisations to be maintained by authorities coming within the Act. The RIPA Coordinating Officer maintains this register.

6.2 Whenever authorisations (including reviews, renewals and cancellations) are issued the authorising officer must (within 7 days of issue) arrange for the document to be sent to the RCO in a sealed envelope marked "Confidential" for the Central Record. Further copies must be placed on the individual case file, retained on the Directorate's Central Record.

Magistrate approvals of authorised applications must be similarly copied and retained.

The diagram below illustrates this part of the procedure.



7. Codes of Practice

As outlined above, there are Home Office codes of practice that expand on this guidance. The Codes are available to staff and members of the public on the Home Office website at https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice.

The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. As stated in the codes, "if any provision of the code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under the 2000 Act, or to one of the commissioners responsible for overseeing the powers conferred by the 2000 Act, it must be taken into account".

Staff should refer to these Codes of Practice for supplementary guidance.

8. Benefits of Obtaining Authorisation under the 2000 Act

8.1 Authorisation of Surveillance and Human Intelligence Sources

The 2000 Act states that

- if authorisation confers entitlement to engage in a certain conduct and
- the conduct is in accordance with the authorisation, then
- it shall be "lawful for all purposes".

However, the opposite is not true – i.e. if you do not obtain the 2000 Act authorisation it does not make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means you cannot rely on any of the benefits and protections RIPA provides.

8.2 The 2000 Act states that a person shall not be subject to any civil liability in relation to any conduct of his which: –

a) is incidental to any conduct that is lawful by virtue of S5(1); and

b) is not itself conduct for which an authorisation or warrant is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

9. Reporting errors

NOTE failure to adhere to the RIPA safeguards can have significant consequences for an affected individual's rights and must be reported to the Investigatory Powers Commissioner.

9.1 The SRO will review the Central Record of authorisations at regular intervals and maintain a log of the findings of those reviews, including whether a relevant error has been identified or authorisation obtained based on incorrect information. A relevant error is any error by the local authority in complying with the RIPA requirements. This would include circumstances where;

- Surveillance or CHIS activity has taken place without lawful authorisation
- There has been a failure to adhere to the safeguards provided in the legislation, or those contained in the Codes of Practice

9.2 If an officer believes or suspects a relevant error has occurred or that authorisation has been obtained based on incorrect information they must report this immediately to the SRO.

9.3 On identifying or receiving a report of a relevant error or that authorisation has been obtained based on incorrect information, the SRO will direct investigation by a nominated officer, and approve the terms of reference

and timescale for that investigation. Where practicable the investigation shall be completed within 10 working days. The report should state the cause of the error, the amount of surveillance or CHIS activity conducted and material obtained or disclosed, any unintended collateral intrusion, the local authority's analysis and action taken, whether any material has been retained or destroyed and action taken to prevent recurrence.

9.4 Where a relevant error is identified the SRO will make a full report to the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than 10 working days (or as agreed with the Commissioner) after it has been identified to the SRO. Where the full report is not available within that timescale, or it is clear that the full report is unlikely to be available within 10 days the SRO will make an initial notification to the Commissioner as soon as reasonably practicable with an estimated timescale for providing the full report and an explanation of the steps being taken to establish the full facts of the error.

10. Oversight and Tribunal

10.1 The Investigatory Powers Commissioner and his Judicial Commissioners are responsible for overseeing the use of investigatory powers by public authorities which include law enforcement, local authorities and other regulators.

10.2 The **Investigatory Powers Tribunal** (**IPT**) is an independent judicial body which hears complaints about surveillance by public bodies. The Tribunal has jurisdiction to consider complaints about the use of surveillance by any organisation, including a local authority, that has powers under the Regulation of Investigatory Powers Act.

10.3 Complaints can be made by persons aggrieved by the council's actions or alleged actions, e.g. a person who believes they have been the subject of directed surveillance. Claims should be brought within one year unless it is just and equitable to extend that.

10.4 Organisations under the IPT's jurisdiction must provide details to the IPT of any activity that is being complained about The IPT's role is to decide whether any surveillance that is being carried out is lawful. The IPT will consider, on a judicial review basis, whether surveillance has been appropriately authorised and conducted in accordance with RIPA requirements.

9.5 The tribunal can order, among other remedies, the quashing or cancellation of any warrant or authorisation and can order destruction of any records or information obtained by using a warrant or authorisation or records of information held by a public authority in relation to any person. The case may currently then be taken on to the European Court of Human Rights in the event of dissatisfaction with the IPT's conclusions.

APPENDIX 1

Definitions from the 2000 Act

- "1997 Act" means the Police Act 1997.
  "2000 Act" means the Regulation of Investigatory Powers Act 2000.

- **"Confidential Material"** has the same meaning as it is given in sections 98-100 of the 1997 Act.

  It consists of: -

  a) matters subject to legal privilege;

  b) confidential personal information; or

  c) confidential journalistic material.

- **"Matters subject to legal privilege"** includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege (see Note A below).

- **"Confidential Personal Information"** is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

  a) to his/her physical or mental health; or

  b) to spiritual counselling or other assistance given or to be given, and which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office (see Note B below). It includes both oral and written information and also communications as a result of which personal information is acquired or created.

  Information is held in confidence if:

  c) it is held subject to an express or implied undertaking to hold it in confidence; or

  d) it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

- **“Confidential Journalistic Material”** includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

- **“Covert Surveillance”** means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place;

- **“Authorising Officer”** For the purposes of authorising directed surveillance under the 2000 Act an “authorising officer” means the person designated for the purposes of section 28 of the 2000 Act to grant authorisations for directed surveillance. (See the Regulation of Investigatory Powers) (Prescription of Officers, Ranks and Positions) Order SI 2000/2417.

- **"Private Information"** defined in Section 26(10) of RIPA as including any information relating to a person's private or family life. This must be broadly interpreted to include an individual's private or personal relationships with others, and family life should be treated as extending beyond the formal relationships created by marriage. Applying a broad interpretation means it may also include business and professional activities.

- **“Working Day”** means any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom.

Note A. *Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.*

Note B. *Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient’s medical records.*

Appendix 4

REGULATION OF INVESTIGATORY POWERS ACT 2000

SOURCE RECORDS REGULATIONS

Particulars to be included in the records relating to each source:

(a) the identity of the source;

(b) the identity, where known, used by the source;

(c) any relevant investigating authority other than the authority maintaining the records;

(d) the means by which the source is referred to within each relevant investigating authority;

(e) any other significant information connected with the security and welfare of the source;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances in which, the source was recruited;

(h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);

(i) the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the source and the demands made of him in relation to his activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by each relevant investigating authority by the conduct or use of the source;

(m) any dissemination by that authority of information obtained in that way; and

(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.