POL00094132

Royal Mail Internal Information
Criminal Investigation Team

6.1 Directed Surveillance

Version 3.0 Final

April 2012

Review Date: April 2013

Ray Pratt
Head of Investigations Policy & Standards
Royal Mail Security
Mobex 5364 3533
Mobile GRO

POL00094132

Contents

POL00094132

Directed Surveillance

1. Introduction

1.1 Directed Surveillance Under RIPA. The Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory framework for the authorisation of Directed Surveillance (DS) by "Relevant Public Authorities". Royal Mail Group Ltd (RMG Ltd) is a Relevant Public Authority (RPA) as a universal service provider, within the meaning of the Postal Services Act 2000, but only when acting in connection with the provision of the universal postal service. This is because the provision of a national postal service is a public function, but all other activities carried out by RMG Ltd are the activities of a private business and as such are outside the authority of RIPA. Parcelforce Worldwide delivery and collection network is not part of the universal postal service and as such DS in investigations into theft from that network fall outside of RIPA.

1.2 Without an appropriate RIPA authority, any DS conducted in connection with the provision of the universal postal service by RMG Ltd, could amount to an unlawful interference with a person's Article 8 Rights, "the right to respect for private and family life" under the Human Rights Act 1998.

1.3 Directed Surveillance Outside of RIPA. It is the policy of RMG Ltd that all cases which require DS should be subject to the same stringent safeguards to ensure consistent evaluation of proportionality and necessity prior to any interference with a person's private or family life. Accordingly the process to obtain DS authority in non-RIPA cases will mirror the processes in RIPA cases.

1.4 Scotland. Investigators conducting investigations in Scotland should note that RMG Ltd is not scheduled as a RPA under the Regulation of Investigatory Powers (Scotland) Act 2000. It is however a RPA in all parts of the United Kingdom under RIPA 2000. The authority under RIPA 2000 which allows DS authorities to extend to Scotland can be found in "The Regulation of Investigatory Powers (Authorisations Extending to Scotland) Orders 2000 & 2007". As such, all RIPA and non-RIPA DS in Scotland should be conducted in accordance with RIPA 2000 and the Covert Surveillance & Property Interference Code of Practice.

1.5 The RIPA 2000 Covert Surveillance & Property Interference Code of Practice (CS&PI CoP) is associated with these Procedures & Standards. Oversight of the conduct of covert surveillance and covert human intelligence sources by public authorities is maintained by The Office of Surveillance Commissioners (OSC). The Surveillance Commissioners website www.surveillancecommissioners.gov.uk, provides advice and guidance for relevant public authorities such as RMG Ltd, with a number of useful links to other relevant sources of information.

1.6 Group Security Forms. The most recent version of the following forms must be used at all times and are available on the Royal Mail Security SharePoint Site.

GS095	Application for authority to carry out Directed Surveillance.
GS095a	Application to review authority to carry out Directed Surveillance.
GS095b	Application to renew authority to carry out Directed Surveillance.
GS095c	Application to cancel authority to carry out Directed Surveillance.
GS096	Authority for 3rd parties to conduct Directed Surveillance.
GS097	Authority Log (record maintained by Authorising Officers).
GS098	Urgent Oral Authorisation Booklet (booklet completed by Authorising Officers).

2. What is Directed Surveillance?

2.1 In order to accurately assess the need for an authority to carry out DS, it is imperative that Investigators have a clear understanding of what constitutes DS. In circumstances whereby the proposed activity does not fall within the definition, then an authority would not be necessary. If there is any doubt as to whether the intended activity constitutes DS, advice must be sought from an Authorising Officer (AO).

POL00094132

Key Accountabilities

Who is accountable?	What do I have to do?	When do I have to do this?	How do I do this?
All members of Royal Mail Security	Ensure you comply with these procedures	Ongoing	As detailed within these procedures

POL00094132

2.2 Directed Surveillance (defined by Section 26(2) of RIPA 2000). Is surveillance which is covert (see 3.1 below) but not intrusive (see 3.2 below) and undertaken:

2.2.1 For the purpose of a specific investigation or a specific operation;

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

2.2.3 Otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practical for an authorisation to be sought for the carrying out of the surveillance.

2.3 Important. The failure to properly categorise what is DS may result in the Human Rights of others being breached and potentially lead to litigation action against the Business and/or individuals. Furthermore, significant and incriminating evidence obtained in such circumstances may be subject to challenge and potentially held as inadmissible in Court (Section 78 Police and Criminal Evidence Act 1984 (PACE)). DS must be authorised as described in Section 4 below.

2.4 Under no circumstances must a third party be asked to carry out any activity that may be construed as DS without the appropriate authority being obtained.

3. Terminology, Definitions and General

3.1 Covert Surveillance (defined by Section 26(9a) of RIPA 2000). Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. (This includes the use of overt CCTV systems for the purposes of a specific investigation or operation).

3.2 Intrusive Surveillance (defined by Section 26(3) of RIPA 2000). Surveillance is 'intrusive' if it is covert surveillance that;

3.2.1 Is carried out in relation to anything taking place on any residential premises or in any private vehicle and

3.2.2 Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

3.3 RMG Ltd has no authority to perform 'Intrusive Surveillance' under any circumstances. It is therefore vital that Investigators understand what constitutes 'Intrusive Surveillance'. Additionally RMG Ltd has no power under the Police Act 1997 to "interfere with property".

3.4 Private information (defined by Section 26(10) of RIPA 2000). Includes information relating to a person's private or family life. This includes an individual's private or personal relationships with others and extends beyond the formal relationships created by marriage.

3.5 Collateral Intrusion (CS&PI CoP 3.8 to 3.10 refer). The term collateral intrusion is used to describe the potential invasion of privacy, of any other persons who are not the subject or target of the surveillance. (See 4.19 to 4.21 below).

3.6 Necessity and Proportionality (CS&PI CoP 3.3 to 3.7 refers). The terms necessity and proportionality have given rise to much debate. There is a common misunderstanding when it comes to differentiating between the two. In the first instance, the AO must believe that the proposed surveillance is necessary for one of the statutory grounds/reasons provided by Section 28(3) of RIPA 2000. RMG Ltd as a RPA is restricted to the use of RIPA 2000 powers for the purpose of "preventing or detecting crime or preventing disorder" only, as set out in Section 28(3b) of the Act.

3.7 Once satisfied that it is 'necessary', in the particular case under investigation, the AO must believe that the proposed activity is in fact 'proportionate' to what it seeks to achieve. This involves balancing the seriousness of the intrusion into the privacy of the target of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

POL00094132

3.8 Guidance on Proportionality is given in the CoP (CS&PI CoP 3.5), as follows. *The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.*

3.9 The following elements of **proportionality** should therefore be considered:

3.9.1 Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

3.9.2 Explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;

3.9.3 Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

3.9.4 Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

3.10 Further explanation and guidance on proportionality is provided at 4.14 to 4.18 below.

3.11 **Confidential Information/Material (CS&PI CoP 4.1 & 4.28 refers).** Is defined as being,

3.11.1 Matters subject to legal privilege, or

3.11.2 Communications between a Member of Parliament and another person on constituency matters. (References to a Member of Parliament include references to Members of both Houses of the UK Parliament, the European & Scottish Parliament and the Welsh & Northern Ireland Assemblies), or

3.11.3 Confidential personal information, such as details of the subject's spiritual, welfare or medical condition, or

3.11.4 Confidential journalistic material.

3.12 If confidential material is acquired or retained during DS which was unplanned then the matter must be reported to the Senior Investigation Manager Policy and Standards on 020 7881 4313. In cases where it is thought likely that as a consequence of DS a person may acquire knowledge of "confidential material", special authorisation would be required. In such cases, the AO would be the Director of Group Security. The processes for the handling, recording, disposal and/or destruction of such confidential material, will be determined when authorised or when retained and this may require advice from the Criminal Law Team (CLT).

3.13 Further explanation and guidance is provided at paragraph 4.22 below.

3.14 **Product of Surveillance (CS&PI CoP 9.5 refers).** There is nothing in RIPA 2000 that prevents material obtained from properly authorised surveillance being used in other investigations or proceedings, (including civil and disciplinary). Investigators must ensure that all evidence and/or intelligence gathered (i.e. the product of the DS operation), is handled, stored or destroyed in accordance with the instructions given by the AO when the surveillance authorisation is cancelled using the GS095c procedure.

3.15 **Authorising Officer.** An AO in respect of DS is deemed by legislation as being a 'Senior Investigation Manager'. Within Royal Mail Group Ltd this is determined as being a Senior Investigation Manager of BPC8 level or above.

3.16 **Note** – In some circumstances, the Director of Group Security may allow persons temporarily promoted to BPC8 level or higher, to be recognised as AO.

3.17 **Durations of Authorisations (CS&PI CoP 5.10 & 5.11 refers).** A written application granted by an AO will cease to have effect (unless renewed) at the end of a period of three months beginning with the day on which it took effect. (See 4.23.12 below). Urgent oral authorisations cease to have effect after 72 hours. (See 3.24 below).

POL00094132

3.18 Note: Once any authority has expired, a new application form GS095 is required.

3.19 Immediate Response. Remember the definition of Directed Surveillance (see 2.2 above), takes account of "an immediate response to events or circumstances", which, by their very nature, could not have been foreseen'. Such 'immediate response' circumstances are **not** 'Directed Surveillance', and would therefore **not** require an Urgent Oral Authority.

3.20 There is no case law to assist in defining when the immediate response ends and an urgent oral authority should be requested. To ensure good governance Investigators should apply for urgent oral authority as soon as it is reasonably practicable, without compromising the quality of the possible evidence.

3.21 Urgent Oral Authorities It is recognised that **urgent** situations will arise whereby it is not possible to prepare and submit a written application to carry out DS. In such situations, an AO may grant oral authority to carry out specific activities. These circumstances are likely to be very few and far between within RMG Ltd.

3.22 Urgent Oral Authority Applications. In circumstances that warrant urgent oral authority, the AO is required to complete an Urgent Oral Authorisation form GS098. An aide memoir to the GS098 has been produced to inform the Investigator of the likely questions that they will be asked. The Applicant must make a written record, as soon as is reasonably practicable, preferably in an official notebook, detailing;

3.22.1 The identities of the subject(s) of the surveillance.

3.22.2 The exact nature of the surveillance operation authorised. (To include details of AO and time authorised)

3.22.3 The reason the AO considered the case urgent.

The applicant must then ensure that all involved in the Surveillance team are briefed on the exact nature and the extent of the surveillance activities authorised and make a written record to this effect.

3.23 Guidance on Urgent Cases is given in the CoP (CS&PI CoP 8.8), as follows; *"A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's own making."*

3.24 Oral authority will cease to have effect after 72 hours from the time the authorisation was granted. For surveillance to continue beyond the 72 hours then authority for renewal must be sought using the form GS095b.

3.25 Note: If as a result of the authority, the operation is resolved, then a cancellation form GS095c must be completed by the Investigator in the case and submitted to the AO as soon as practicable.

4. Written Applications for authority to carry out Directed Surveillance

4.1 Directed Surveillance, as defined at 2.2 above, can only be authorised if the AO considers it to be both **necessary** and **proportionate** to preventing or detecting crime, and that issues of both **collateral intrusion** and **confidential material** have been considered.

4.2 Note: It is useful to remember that the GS095 application, must provide the AO with accurate information that determines – Who, What, Where, When, Why and How.

4.3 The following paragraphs aim to provide advice and guidance in general terms. Clearly it is not possible to take every eventuality into account and any uncertainty should be discussed with an AO before action is taken. Additionally Investigators should remember that each application should be considered in isolation and as such they should avoid "cut and paste" when completing applications.

POL00094132

4.4 Part 1 – Application for authority to carry out Directed Surveillance.

4.4.1 The 'Authorisation No.' is a unique number generated by the AO. In RIPA applications it will consist of the Authorising Officer's Security Identity Card number, a consecutive running number of applications considered by the AO for that calendar year and finally the current year. In non-RIPA cases the number will commence "NR". **Important note.** RIPA and non-RIPA application numbers must be totally separate. For example if the Authorising Officer's security card number is 456 the first RIPA Application will be 456/001/2009, the second 456/002/2009. The first non-RIPA application will be NR456/001/2009 and not NR456/003/2009.

4.4.2 The Investigator must indicate whether the application for DS is in accordance with RIPA 2000, in that it is connected with the provision of the Universal Postal Service. (If in doubt the matter should be discussed with an AO)

4.4.3 The 'Case Reference' is that raised by the SIMS system. The 'Event Number' should only be used if unavoidable.

4.5 Part 2 – Identify on which grounds the Directed Surveillance is necessary. (CS&PI CoP 3.3 refers)

As detailed at 3.6 above, the AO must believe that the proposed surveillance is necessary. The only statutory grounds under RIPA 2000, for which it is necessary for RMG Ltd as a RPA to conduct DS, is for the purpose of preventing or detecting crime. This will also be the only reason for non-RIPA DS applications. The form already details this reason.

4.6 Part 3 – The Identities, where known, of those to be subject of the Directed Surveillance. (CS&PI CoP 5.8 refers)

4.6.1 This part is largely self-explanatory. Where more than two subjects are involved, additional rows should be created.

4.6.2 If the identity of a subject is not known, it is permissible to modify the sub-headings to cater for the circumstances (e.g. 'description' or 'other info')

4.7 Part 4 – Describe the crime under investigation, the evidence gathered, how the suspect is implicated and the reasons why the authorisation is necessary in this particular case.(CS&PI CoP 5.8 refers)

Provide a concise explanation including;

4.7.1 What crime is being investigated (e.g. theft of mail at a particular Delivery Office (DO) – contrary to S1 of the Theft Act 1968).

4.7.2 How the criminal activity came to light (e.g. customer complaints or debris found).

4.7.3 Evidence of current criminal activity (e.g. continuing loss levels).

4.7.4 What evidence links the subject with the current criminal activity (e.g. analysis or Due Course Delivery Officer (DCDO)).

4.7.5 What evidence is the DS expected to provide.

4.7.6 How the evidence or information being sought will materially assist the investigation.

4.8 **Remember:** The purpose of your submission is to justify the need to carry out the DS. Avoid the use of unnecessary detail and any specific investigation methodology. You will have the opportunity elsewhere to demonstrate how thorough your investigation has been. In completing the application Investigators should avoid vague terms that raise questions for the reader and avoid/clarify any 'business' jargon.

4.9 Part 5 – During the course of the investigation has further information or intelligence been obtained from the National Intelligence Database or the ISR that the AO should be made aware of?

Under no circumstances must any information be included in the application that could identify an individual registered on the Intelligence Source Register (ISR) or a Police Covert Human Intelligence Source (CHIS). In these situations only the ISR/CHIS unique reference number (URN) must be stated. The URN will allow the AO to ascertain and examine the information concerned.

4.10 Part 6 – Describe the surveillance operation to be authorised including equipment to be used.

POL00094132

Whilst being succinct and to the point, provide an overview of the proposed operation. Specific detail of the operation and who is doing what and how should not be included. Limit your description to a general summary of what the operation will involve and the potential for developments in the case. This should include;

4.10.1 Anticipated times and expected duration of surveillance activity.

4.10.2 Number of Investigators involved.

4.10.3 Where the proposed surveillance is to take place, e.g. DO, delivery route to home address and any deviation from this. If relevant, Investigators should allow for developments in terms of potential new subjects, locations and tactics. See paragraph 4.11 below.

4.10.4 Premises to be used for the surveillance (do not identify any confidential locations). See paragraph 6.1 below dealing with the confidentiality of observation points in accordance with R v Johnson.

4.10.5 Number of vehicles to be utilised.

4.10.6 Equipment to be utilised (e.g. CCTV, still cameras, binoculars, camcorder and electronic tracking devices) including the scope and coverage if this is applicable.

4.10.7 In cases which require a covert camera(s) to be installed it is important that precise detail of the extent of the coverage is contained in the application. Where possible best practice will be to provide the AO with a floor plan/sketch of the area to be covered by the covert camera(s). See paragraph 4.19 in respect of collateral intrusion and Part 13 at paragraphs 4.25 & 4.26 below in respect of the installation engineer's role.

4.11 The Developing Operation. Where appropriate the original application should include details of potential developments in the surveillance operation which allows Investigators to act quickly, without losing sight of a suspect(s) and risking the continuity of evidence. For example, where the subject is not known, or there is a possibility that additional subjects may be involved, the application should be worded in such a way that it allows for the operation to continue and/or expand should a subject or additional subjects be identified. Unless the continued activity leads to an apprehension (in which case a cancellation is likely to be appropriate) a review should be submitted as soon as reasonably practicable recording the details and impact of the development. This must be done and authorised before further DS activity takes place.

4.12 Reviews and renewals should not add new suspects, locations or tactics to the authorisation unless these were clearly stipulated as potential fully justified additions within the wording of the original application. If not a fresh application must be submitted.

4.13 Part 7 – What is the defined objective of the Directed Surveillance? (CS&PI CoP 5.8 refers)

The defined objective may be;

4.13.1 To gather evidence which will prove or disprove the subject's involvement in the crime under investigation or,

4.13.2 To identify the person responsible for crime under investigation.

4.14 Part 8 – Explain why this Directed Surveillance is proportionate to what it seeks to achieve. (CS&PI CoP 3.6 refers)

You will have already explained the 'need' for the proposed surveillance, in terms of evidential value, in Parts 2 & 4 of the application. You are now required to demonstrate that the proposed surveillance is in fact proportionate. In other words, that the potential intrusion on the subject's privacy, is fair and reasonable in the circumstances. To reiterate the explanation at 1.2 above – the focus of this legislation is one of fairness and regard for an individuals 'right to respect for private and family life'.

4.15 The following points may help position what explanation is required;

4.15.1 The proposed activity must be proportionate when balanced against the seriousness of the offence and the defined objective.

4.15.2 The level of 'intrusion' on the subject of the surveillance, and others, is the key issue.

4.15.3 The level of 'intrusion' must be kept to a minimum.

POL00094132

4.16 Demonstrate that you have considered;

- 4.16.1 Other ways or methods of obtaining the required evidence, which would not be as intrusive, and why they have been discounted.
- 4.16.2 Why there is a need for adopting a 'covert' means of securing the evidence, rather than a more open, less intrusive approach and is this most appropriate.
- 4.16.3 The subject's expectation of privacy within the areas they will be under surveillance.
- 4.16.4 The scale of the operation and size of the surveillance team compared with the gravity and extent of offending.
- 4.16.5 How all of the above points are proportionate when balanced against the objective.

4.17 In relation to point 4.16.3 above, Investigators may consider the impact of CCTV and signage on the level of privacy expected by the subject. Clearly a higher expectation of privacy would exist in areas such as welfare rooms, prayer rooms, locker rooms and vehicles. You should provide increased justification for the intrusion if this is the case.

4.18 In other words the Human Rights of others are being preserved by keeping the surveillance to a minimum whilst being sufficient to achieve its purpose in obtaining the evidence or information necessary to support the investigation.

4.19 **Part 9 – Supply details of any potential collateral intrusions and what precautions you will take to minimise or avoid this happening. (CS&PI CoP 3.8 to 3.11 refers)**

As defined at 3.5 above, collateral intrusion is the 'incidental invasion of the privacy of those not the direct target of surveillance' and understandably the applicant must demonstrate that the potential for this happening has been considered and measures taken to minimise it.

4.20 Provide an assessment of the risk of collateral intrusion by;

- 4.20.1 Outlining who may be affected and why.
- 4.20.2 How it is intended to ensure that any unavoidable collateral intrusion is kept to a minimum.

4.21 Note: In circumstances whereby an area is targeted with no specific suspect, collateral intrusion does not apply to those working within that area.

4.22 **Part 10 – Confidential Information – Is it likely that the Directed Surveillance will result in the acquisition of any of the following? (CS&PI CoP Chapter 4 refers)**

Clearly indicate either 'Yes' or 'No' against each of the four types of information listed. In the event of the answer to any of the questions being 'Yes', you must provide a description of the material/information concerned and explain how it will be handled. Advice on this matter may be sought from the CLT. Where there is any intention or likelihood of acquiring such information, the level of authority rests with the Group Security Director.

4.23 **Part 11 – Authorising Officer's Statement. (CS&PI CoP 5.8 refers)**

If granting the application, the AO concerned is required to provide a clear statement to that effect. The statement is likely to include a summary of;

- 4.23.1 The authorisation is under Section 28 (3b) RIPA 2000, namely for the purpose of preventing or detecting crime or of preventing disorder.
- 4.23.2 Who the subject is, if known.
- 4.23.3 Why the proposed activity is necessary.
- 4.23.4 What activity and equipment may be involved? In cases involving the installation of covert camera(s) the AO must include precise instructions as to the extent of the coverage of the camera(s) and replicate this within Part 13 of the form. (See paragraphs 4.25 to 4.28 below).
- 4.23.5 Where the proposed surveillance is to take place.
- 4.23.6 When the proposed surveillance is to take place.
- 4.23.7 The objective of the operation.

POL00094132

4.23.8 Whether the proposed activity is proportionate.

4.23.9 What collateral intrusion may be involved and how this will be minimised. Where covert CCTV is to be installed AO's should give due consideration to the potential technical difficulties in limiting the coverage to what is authorised. (Details pertaining to the installation of covert CCTV need to be replicated in Part 13).

4.23.10 The likelihood of acquiring confidential material.

4.23.11 What is authorised in respect of potential developments in the case (See paragraph 6.11 above). This is to include the activities authorised should new subjects, locations or tactics be identified and any conditions imposed in the authorisation in respect of the development.

4.23.12 A written authorisation will cease to have effect (unless renewed) at 23.59hrs at the end of a period of three months, less one day, from when it took effect. For example, a written authorisation granted on the 24th April will cease at 23:59 hours on the 23rd July.

4.24 Part 12 – Authorising Officer.

To be completed by the AO.

4.25 Part 13 – Installation of Covert Cameras Authorising Officer.

In order to ensure that an installation engineer does not unwittingly install covert equipment that goes beyond the extent of DS authority they must be fully briefed on the coverage of such equipment. The installation engineer should be shown this part of the form only and be given precise instructions on what has been authorised. Where available this may include sight of a floor plan/sketch of the area to be covered.

4.26 The engineer is required to sign a declaration to the effect that they have installed the covert camera(s) in accordance with the parameters of the authorisation.

4.27 Part 14 – Investigator In Charge (IIC) Declaration.

The IIC must provide all members of the operational surveillance team with a copy of the AO statement prior to any surveillance and must sign the certificate to this effect. If new members join the team after the briefing they must also be given a copy of the AO statement before they commence surveillance and a note made by the IIC.

5. Reviews, Renewals and Cancellations

5.1 Reviews of Authorisations. Every authorisation to carry out DS must be regularly reviewed by an AO who will assess the need for the Surveillance to continue. Reviews should be submitted if there have been any significant changes;

5.1.1 In relation to the subject, method, equipment or scope of the surveillance.

5.1.2 Regarding the proportionality of the operation.

5.1.3 To the position in respect of collateral intrusion or acquisition of confidential information. Or;

5.1.4 At least every month or any shorter period stipulated by the AO. Such reviews must be submitted to the AO 2 days prior to the designated review date, which will have been determined at the time of authorisation.

5.2 Timely Reviews. If a DS authority has been granted which allows for development in the operation (see paragraph 4.11 above) then a timely review will be necessary to advise the AO of specifics of the development, any changes to the scope and methodology of the operation and any other changes in accordance with paragraph 5.1 above.

POL00094132

5.3 General Reviews & Renewals. All review, renewal and/or cancellation requests must quote the original authority number for the DS. It is also preferable to submit such requests to the AO who authorised the DS in the first instance. Should changes in the authority be made by an AO as a result of a review then these changes should be highlighted in the next renewal. All written reviews and renewals must include the dates of all previous reviews or renewals. (See 7.3 below in relation to submission and recording processes).

5.4 Renewal of Authority (CS&PI CoP 5.10 refers). As detailed at 4.23.12 above a written authorisation will cease to have effect (unless renewed) at 23.59hrs at the end of a period of three months, less one day, from when it took effect. The example in paragraph 4.23.12 above showed that a written authorisation granted on the 24th April will cease at 23:59 hours on the 23rd July. If a renewal is authorised, this will have taken effect at 23.59 hours on 23rd July. To request that an authority is renewed, a completed form GS095b must be received by the AO 6 days prior to the date on which the authorisation period comes to an end.

5.5 Content of a Renewal (CS&PI CoP 5.15 refers). The questions at parts 3 to 6 of the Renewal Application Form GS095b incorporate specific requirements determined by the CoP. Authorisations may be renewed more than once if necessary.

5.6 Authorising Officer (CS&PI CoP 5.13 refers). When considering the application for the DS to continue, the AO must be satisfied that it is still necessary 'for the purpose for which it was given'.

5.7 Reviews and Renewals of Authority to Conduct Directed Surveillance. If as a result of the submission of a review or a renewal there is a change to the subject, method, equipment or scope of the surveillance authority then all the Surveillance Operational Team members should be provided with a copy of the relevant AO Statement. Part 8 – "The Investigator in Charge Declaration" should be completed on both the GS095a & GS095b following a review or renewal of an application.

5.8 Cancellation of Authority (CS&PI CoP 5.17 & 5.18 refers). In circumstances whereby the DS no longer meets the criteria upon which it was authorised, it must be cancelled (e.g. subject apprehended or no longer has viable access to relevant property).

5.9 In order to protect the Human Rights of those who have been the subject of the surveillance, either directly or indirectly, all surveillance activity must cease forthwith and a completed form GS095c submitted to the AO as soon as practicable. In part 3 of the GS095c, it must be made clear what material/evidence was acquired as a consequence of the surveillance and how it is proposed to deal with it. This may be to use it in the criminal process, destroy it, store it, or to make it available for another process such as conduct or a tribunal.

5.10 Product of Surveillance. When cancelling the surveillance authority the AO will provide instructions regarding the handling and disposal of such material/evidence.

6. Confidentiality of Observation Points and Authority for 3rd Party Surveillance from or within Royal Mail Group Ltd Premises

6.1 Confidentiality of Observation Points, R v Johnson. R v Johnson is case law which deals with the confidentiality of observation points (OP). As a result of "Johnson", Judges can rule that officers do not answer specific questions which may reveal the location of an OP, if it is thought that to do so could result in reprisals against the occupants. Before a Judge can make such a ruling certain actions have to take place. In a RMG Ltd led investigation these would be as follows;

6.1.1 An Investigation Team Manager (ITM) or above must be able to testify that they visited the OP before it was used and spoke with the occupants. During the visit they established the occupant's attitude to firstly what their premises were to be used for and secondly, the possible disclosure of the location of the OP in Court, leading to their identity being revealed;
and

POL00094132

6.1.2 A Senior Investigation Manager (SIM) of BPC8 or above must be able to testify that, in the event of a trial, immediately prior to it commencing, they will visit the OP to establish firstly, whether the occupiers are the same as when the observations took place and secondly, whether they were or were not, their attitude to the possible disclosure of the OP leading to their identity being revealed.

If Investigators in RMG Ltd led investigations are intending to use OP, which may result in reprisals against the occupants, then they should ensure that the "Johnson" actions are carried out. In Police or other RPA cases the process is the same but instead of an ITM it should be an officer preferably a Sergeant or above (or equivalent) and for a SIM a Chief Inspector or above (or equivalent).

6.2 Police Led Operations. On occasions the Police or other RPA wish to carry out DS using RMG Ltd premises or other equipment. The management of the use of such premises or equipment is controlled by means of the completion of the Authority for 3rd Parties to Conduct Surveillance Form GS096. The following paragraphs aim to provide advice and guidance in general terms on the completion of the GS096.

6.3 Part 1 – To be completed by an officer involved in the surveillance from the 3rd party concerned.
This section is for completion by an officer in the 3rd party organisation involved. They are required to certify that the DS is lawfully authorised and that they have read the guidance notes on the form.

6.4 Part 2 – To be completed by a Royal Mail Group Ltd Investigator.
The Investigator facilitating the application should ensure that any use of our premises or equipment is in accordance with the legal requirements of RIPA and as such must see the part of the authority (redacted if necessary) which deals with the use of our premises and equipment. Without sight of the relevant part of the authority RMG Ltd could be susceptible for damages should the subject of the surveillance claim violation of their Human Rights. If the 3rd party refuses to disclose the relevant information advice must be sought from an AO.

6.5 Investigators should certify that they have read, understood and considered the guidance notes detailed on the form and then send a copy of the form to an AO in their line.

6.6 Part 3 – To be completed by a Royal Mail Group Ltd Authorising Officer.
Any 3rd party application has to be authorised by a RMG Ltd AO. The AO must consider the Health and Safety of all RMG Ltd employees, visitors and customers and whether R v Johnson should be invoked. They should also consider if there are any other implications for the business.

6.7 The details on the GS096 should be recorded on the GS097, Record of Authorisations by the Authorising Officer. The original GS096 should then be returned to the Investigator concerned.

6.8 A copy of the GS096 should be provided to the Prosecution Support Office (PSO) see 7.2 – 7.3 below. The '3rd party' concerned may be given the 'original' for their records and disclosure purposes.

6.9 Investigators must ensure that whilst on RMG Ltd premises the 3rd party concerned fully complies with our Health and Safety requirements.

7. Submissions and Authorisation Procedure

7.1 Central Record of Authorisations (CS&PI CoP Chapter 8 refers). In compliance with RIPA 2000, and our status as a RPA, the PSO maintains a centrally retrievable record, which is regularly updated whenever an application is made, authorised, reviewed, renewed or cancelled.

7.2 In addition to maintaining the centrally retrievable record, the PSO are responsible for monitoring our compliance with the requirements of RIPA in relation to applications, reviews, renewals and cancellations. Contact details;

Email: RMLS_RIPA
Post: Prosecution Support Office (RIPA)

POL00094132

Room 1D 93
Leeds Mail Centre
Leodis Way
LEEDS
LS10 1AZ

7.3 Written Application Process.

7.3.1 All written DS applications will be sent electronically to the PSO using the email address above. The PSO will then allocate the application in sequence to an AO. Investigators should endeavour to allow a minimum of three days for the authorisation to be considered and returned. If the circumstances of the case require authority within 3 days, the applicant should contact their own Head of Investigation in the first instance. If urgent, oral applications can be made to any Senior Investigation Manager of BPC 8 or above. (See paragraphs 3.19 and 3.22 above.)

7.3.2 AO considers application and completes Parts 11, 12 and, if relevant, 13.

7.3.3 AO prints, signs and retains relevant 'authorisation' page.

7.3.4 AO sends updated version of form by email to applicant and to the PSO using the RMLS_RIPA email address as notification of decision.

7.3.5 If covert CCTV Camera(s) is to be installed the Investigator fully briefs the installation engineer. When installed the engineer completes Part 13.

7.3.6 Following the completion of Part 14, the IIC Declaration, the form should be returned to the AO by hand or Special Delivery (SD).

7.3.7 AO associates 'authorisation' page with application and sends it to the PSO at the address detailed at 7.2 above.

7.3.8 The PSO retains original document and sends 2 copies to the applicant.

7.3.9 AO maintains a record of all applications on form GS097.

7.4 Important Note: A written GS095 RIPA application is not lawfully authorised until the signature of an AO is appended

7.5 Process – Urgent Oral Authorities The process for an Urgent Oral Authority is as follows;

7.5.1 Applicant relates circumstances to AO and requests Oral Authorisation. The AO records details in an Urgent Oral Authorisation Booklet GS098.

7.5.2 AO considers circumstances and advises applicant of decision.

7.5.3 AO advises applicant what, if any, activity is authorised and its parameters.

7.5.4 Applicant makes written record (using official notebook where possible) of:

a. The identities of the subject(s) of the surveillance.

b. The exact nature of the surveillance operation authorisation. (To include details of AO and time authorised.)

c. The reason the AO considered the case urgent.

d. The fact that all Investigators involved in the surveillance operation have been briefed on the exact parameters of the surveillance authority.

7.5.5 A photocopy of this written record must be sent to the PSO at the address detailed at 7.2 above for association with the GS098 completed by the AO.

7.5.6 AO maintains a record of all applications on form GS097.

7.5.7 The GS098 Urgent Oral Booklet is forwarded to the PSO again at the address detailed at 7.2 above.

7.5.8 PSO associates the applicants note with the original GS098 and sends 2 copies to the applicant

7.6 Important Note: As at 3.24 above, Urgent Oral authorisation must be renewed within 72 hours

8. General

8.1 Any unauthorised surveillance activity identified by Line Managers, Heads of Investigations, Casework Managers or the CLT etc, must be reported to the Policy, Standards & Investigation Support Manager.

POL00094132

8.2 All completed DS forms are considered to be 'disclosable material' and will be made available to the Defence.

8.3 The IIC of any surveillance operation is responsible for ensuring that all members of the surveillance team are fully briefed on the subject, scope and method of the surveillance operation prior to any surveillance commencing.

POL00094132

Change Control

Status	Final
Version	3.0
Owner	Ray Pratt
Author	Michael F Matthews
Release Date	April 2012
Document Privacy	Internal

Authorisation

Title	Name	Signature	Date
Security	Ray Pratt		April 2012

Distribution List

Name	Version	Date
All Royal Mail Security via Security Sharepoint	V1	Apr 2011
All Royal Mail Security via Security Sharepoint	V2	Jul 2011
All Royal Mail Security via Security Sharepoint	V3	Apr 2012

Documentation History

Issue	V.1	V2	V3		
Status	Final	Final	Final		
Release Date	Apr 2011	Jul 2011	Apr 2012		
Effective From	Apr 2011	Jul 2011	Apr 2012		

Document Change History

Issue / Version	Summary of Change
V1	Document Produced in RM Format
V2	Central Records Transferred to the PSO
V3	Annual Review and References to Post Office Ltd removed

Glossary

POL00094132

Abbreviation or Term	Meaning
RIPA 2000	The Regulation of Investigatory Powers Act 2000
DS	Directed Surveillance
RMG Ltd	Royal Mail Group Limited
RPA	Relevant Public Authority
CS&PI	Covert Surveillance and Property Interference
OSC	Office of the Surveillance Commissioners
AO	Authorising Officer
PACE	Police and Criminal Evidence Act 1984
CLT	Criminal Law Team
URN	Unique Reference Number
SIMS	Security Information Management System
PSO	Prosecution Support Office
DO	Delivery Office
DCDO	Due Course Delivery Officer
ISR	Intelligence Source Register
CHIS	Covert Human Intelligence Sources
IIC	Investigator in the Case
ITM	Investigation Team Manager
SIM	Senior Investigation Manager
SD	Special Delivery
OP	Observation Post

Document Summary

If you have any queries please contact:

Mick F Matthews
Royal Mail Security
6A Eccleston St
LONDON
SW1W 9LT

Postline: GRO
STD:
E mail GRO

POL00094132