POL00104796

ROYAL MAIL CORPORATE SECURITY – PROCEDURES & STANDARDS

SURVEILLANCE	P&S Doc. 4-X

1. PURPOSE.

The aim of this document is to provide Investigators within the Royal Mail Group, with clear guidance concerning the required Procedures & Standards relating to surveillance.

CONTENTS OF DOCUMENT - by Section

2. INTRODUCTION

2.1 **Background**
The Regulation of Investigatory Powers Act 2000 (RIPA) brought about statutory controls governing the deployment of surveillance, and the equipment used, in relation to 'Directed' and 'Intrusive' surveillance.

2.2 The Act applies to the Police and Designated Public Authorities. As Royal Mail Group (including Post Office Limited) is a Designated Public Authority for the purposes of surveillance we are required to comply with the Act.

2.3 Where the surveillance is likely to interfere with a persons 'right to respect for private and family life' guaranteed under Article 8 of the European Convention on Human Rights, obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse. (Covert Surveillance – Code of Practice Section 2.1 to 2.3 refers)

2.4 The Covert Surveillance – Code of Practice for England, Wales and Northern Ireland are available on the Home Office – Security website. The Codes of Practice for Scotland can be found at www.scotland.gov.uk

The Office of Surveillance Commissioners aim is to provide effective and efficient oversight of the conduct of covert surveillance and covert human intelligence sources by public authorities. The OSC website – www.surveillancecommissioners.gov.uk, provides advice and guidance for public authorities such as ourselves, with a number of useful links to other relevant sources of information.

2.5 **Corporate Security Forms** – available on the Corporate Security Database.

Form No.	Description

POL00104796

ROYAL MAIL CORPORATE SECURITY – PROCEDURES & STANDARDS

CS095	Application for authority to carry out directed surveillance
CS095A	Authority for 3rd parties to conduct directed surveillance (RM/PO premises)
CS095B	Record of application for urgent oral authorisation to carry out directed surveillance
CS095C	Record of authorisation following urgent oral authority to carry directed surveillance
CS096	Application to renew authority to carry out directed surveillance
CS096A	Application to cancel/review authority to carry out directed surveillance
CS097	Authority Log (record maintained by authorising officers)

POL00104796

3. RIPA TERMINOLOGY & DEFINITIONS

3.1 **General observation** (Covert Surveillance – Code of Practice Section 1.8 refers)

On a daily basis, normal business operations are observed under the provisions of the Data Protection Act 1998. Such observation may involve the use of overt CCTV cameras, watching galleries and/or other equipment, such as binoculars, to merely reinforce normal sensory perception. This is not in itself directed surveillance, which is defined at 3.3 below.

Note: The failure to properly categorise what is 'general' and 'directed' surveillance may result in the human rights of others being breached and potentially lead to litigation action against the Business and/or an individual(s). Furthermore, significant and incriminating evidence obtained in such circumstances may be subject to challenge and potentially held as inadmissible in court (S78 PACE). Advice must be sought from an Authorising Officer if there is any doubt as to whether the intended observation goes beyond 'general'.

3.2 **Covert Surveillance** (Covert Surveillance – Code of Practice Section 4.2 refers)
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.

3.3 **Directed Surveillance** (Covert Surveillance – Code of Practice Section 4.1 refers)
Surveillance is 'directed' if it is **covert but not intrusive**, and is undertaken:

- For the purpose of a specific investigation or a specific operation;
- 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**
- Is not as an immediate response to events or circumstances, which, by their very nature, could not have been foreseen. For example, spotting something suspicious and continuing to observe it in circumstances which would otherwise make seeking authorisation under the Act unreasonable (See 6.1-6.6 below – Urgent oral authorities)

Note – Directed surveillance must be authorised as described at 4.1-4.11 below.

3.4 **Intrusive Surveillance** (Covert Surveillance – Code of Practice Section 5 refers)
Royal Mail Group has **no authority under RIPA** to perform 'Intrusive' surveillance under any circumstances. It is vital that Investigators understand what constitutes intrusive surveillance.

Surveillance is 'intrusive' if it is covert and

- Carried out in relation to anything taking place on residential premises or in a private vehicle **and**
- Involves the presence of an individual on the premises or vehicle or is carried out by a

POL00104796

surveillance device

3.5 **Collateral Intrusion** (Covert Surveillance – Code of Practice Section 2.6 – 2.10 refers)
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.

This is discussed in more detail at 4.7 below.

3.6 **Necessity and Proportionality** (Covert Surveillance – Code of Practice Section 2.4 – 2.5 refers)
The 2000 Act requires that the person granting the authorisation believe it is necessary, in the circumstances of the particular case, for one or more of the statutory grounds in section 28(3) and if this is the case, that the activities are proportionate to what is sought to be achieved by carrying them out. The term 'proportionate' refers to the level of 'intrusion' on the subject of the surveillance, **not** the seriousness of the offences. This is discussed in more detail at 4.6 & 4.8 below.

3.7 **Confidential Information/Material** (Covert Surveillance – Code of Practice Section 3.1-3.2 refers)
Confidential Information/Material consists of:

- Matters subject to legal privilege
- Confidential personal information
- Confidential journalistic material

In cases where the likely consequence of 'directed' surveillance would be for any person to acquire knowledge of 'confidential material', special authorisation would be required. In such cases, the Authorising Officer would be the Director of Security. The processes for the handling, recording, disposal and if need be the destruction of such confidential material, will be agreed when authorisation was granted.

3.8 **Product of Surveillance**
There is nothing in the '2000' Act that prevents material obtained from properly authorised surveillance being used in other investigations. Investigators must ensure that all evidence and/or intelligence gathered (i.e. the product of the directed surveillance operation), is handled, stored or destroyed in accordance with Corporate Security Procedures & Standards – Disclosure of Unused Material, CPI Act 1996.

3.9 **Authorising Officer**
An Authorising Officer in respect of directed surveillance is deemed by legislation as being a 'Senior Investigation Officer'. Within Royal Mail Group this is determined as being a Senior Manager of BPC8 level or above, within Corporate Security.

Note – In some circumstances, the Director of Security (or Head of Security) may allow persons temporarily promoted to BPC8 level or higher, to be recognised as Authorising Officers.

3.10 **Durations of Authorisations** (Covert Surveillance – Code of Practice Section 4.19 refers)
A **written** authorisation granted by an authorising officer will cease to have effect (unless renewed)

POL00104796

at the end of a period of **three months** beginning with the day on which it took effect.

Urgent Oral Authorisations cease to have effect after **72 hours** and involve a different process. This is discussed at 6.1-6.6 below.

Note: Once an authority has expired, a new application form CS095 is required.

3.11 **Reviews/Renewals/Cancellations**
Explanation of the processes in respect of reviews, renewals and the cancellation of authorities to carry out directed surveillance, are found at 5.1-5.4 below.

3.12 **Covert Human Intelligence Source (CHIS) /Confidential Witnesses** – the CS Procedures & Standards - Informants (CSD under Gathering Intelligence Data) also refer.

When applying for authority to carry out directed surveillance, it is not appropriate to make any reference to confidential witnesses or Police CHIS. The expression 'Information received, code *XXX...*' must be used. The code will refer to a unique reference number on the CS Information Source Register.

To place individuals, who wish to remain anonymous, on the 'Confidential Witness Register', contact the Corporate Security Helpdesk.

4. APPLYING FOR AUTHORITY TO CARRY OUT DIRECTED SURVEILLANCE

4.1 Directed surveillance, as defined at 3.3 above, can only be authorised if the Authorising Officer considers it to be both necessary and proportionate to the investigation, or prevention of crime, and that issues of both collateral intrusion and confidential material have been considered.

The Covert Surveillance - Code of Practice Section 4 refers.

Note: It is useful to remember that the CS095 application, must provide the Authorising Officer with accurate information that determines - Who, What, Where, When, Why and How.

4.2 **Part 1 of the CS095 'Application for authority to carry out directed surveillance'** is self explanatory, however the following points provide clarification;

- The 'Project Number' is that raised by the SIMS-WMS system (not the Event number). If the project number is not known and cannot be determined at the time, the applicant must update the relevant Authorising Officer immediately the relevant number is established/generated.
- The 'Authority Ref. No.' is a unique number issued by the Authorising Officer. It will consist of the Authorising Officer's RM Security Identity Card number, then a consecutive running number issued by the Authorising Officer for that calendar year and finally the current year.
- The 'Date and Time of Application' details precisely when the application is made, and must be completed on every occasion. This is of particular importance when an oral authority in respect of the activity has previously been refused.

POL00104796

4.3 **Part 2 - Details of suspected offence(s) being investigated or prevented including progress of the investigation.**

- Be clear about what offence/s you are investigating and mention how the matter came to light.
- Avoid trying to detail the entire investigation, sum up the present situation.
- Be clear about how the suspect is implicated
- Avoid vague terms that raise questions for the reader
- Clarify any 'business' jargon i.e. Special Delivery Work Area (SDWA) or YORK (equipment designed to facilitate the handling and movement of postal packets)
- Only refer to confidential witnesses in the terms described at 3.12.

4.4 **Part 3 - Is there any requirement for 'testing' to take place?**
This is a Yes/No answer, the details of which must be furnished within Part 4 of the form.

4.5 **Part 4 - Detail the surveillance activity to be undertaken including use of equipment**

Describe in detail the surveillance operation to be authorised and expected duration, including the resource, premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

4.6 **Part 5 - Explain how the proposed activity is necessary to advance the investigation. (Include any alternative investigative methodologies considered and why they were discounted.)**

- It is likely that the statutory grounds for necessity under section 28(3) of the 2000 Act will be for the prevention/detection of crime.
- Explain what evidence or information is being sought from the surveillance and how this will materially assist the investigation.
- Make it clear to the Authorising Officer that this 'intrusion' on the subject is necessary. Support the application by demonstrating that other means of securing the required evidence have been duly considered and why they have been discounted.
- Matters concerning the RM conduct code, brand, profitability etc, are not relevant to the necessity of the activity.

4.7 **Part 6 - Collateral Intrusion; indicate any potential for collateral intrusion on persons other than those targeted. Outline the plan to minimise collateral intrusion.**

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.

- Outline who may be affected and how it is intended to ensure this is kept to a minimum.
- Explain why the intended size of the surveillance team is necessary.
- If the target is an 'area' with no specific suspect, collateral intrusion does **not** apply to those working within that area.

4.8 **Part 7 - Explain why the proposed activity is proportionate in the circumstances of the case. (Detail the potential level of intrusion, including expected level of privacy, balanced against the needs of the**

POL00104796

operation).

As defined at 3.6 above, 'proportionate' refers to the level of intrusion on the subject being appropriate. Proportionality in this context does **not** refer to the seriousness of the offences; it refers to the level of 'intrusion' on the subject of the surveillance and requires a demonstration of how this has been/will be kept to a minimum.

The Covert Surveillance – Code of Practice (section 2.5) explains proportionality saying: –

"Then, if the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against ***the need for the activity*** *in operational terms. The activity* ***will not be proportionate*** *if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair."*

- Make a statement to show that the operation has a defined objective and is not a 'fishing trip'.
- If appropriate, demonstrate your understanding/recognition that, in some locations, such as welfare rooms or prayer rooms, there is a natural expectation of a higher level of privacy. Provide increased justification for the intrusion if this is the case.
- Conversely, there is a lower expectation of privacy in environments with overt CCTV supported by appropriate signage.
- Be aware that an excessive number of people involved in the surveillance operation may not be proportionate.

4.9 **Part 8 – Confidential Material; indicate the likelihood of acquiring any confidential material.**

As outlined in the definition at 3.7 above, a higher level of authority (Director of Security) will be necessary, if the acquisition of confidential material is likely. Furthermore, the CS Performance & Planning Manager is required to notify the Office of the Surveillance Commissioner.

4.10 **Part 9 - Particulars of the identity/ies, where known, of those to be the subject(s) of the directed surveillance. (Provide details of all known subjects)**

This is self-explanatory.

4.11 **Part 10 – Anticipated Start Date: & Time:**

Proposed commencement of surveillance operation. Use 24 hour clock (00:00 hours)

5. REVIEWS, RENEWALS AND CANCELLATIONS OF SURVEILLANCE AUTHORITIES

5.1 All review, renewal and/or cancellation requests must quote the **original authority number** for the directed surveillance. In the case of reviews and renewal applications, it is suggested that, for the

POL00104796

purpose of continuity, the dates of any previous reviews and/or renewals are included.

5.2 **Review of Authorisation** (Code of Practice Section 4.21 refers)
Every authorisation to carry out directed surveillance must be regularly reviewed by an Authorising Officer to assess the need for the surveillance to continue. Reference must be made to

- Any changes in circumstances influenced by information received or evidence gathered since the initial application (or most recent review/renewal).
- The continued necessity and proportionality of the Directed Surveillance.

A completed form **CS096A** must be submitted to the Authorising Officer prior to the designated review date.

Whilst there is a minimum requirement that such reviews are carried out at least every month during the three month period that the authority is effective, the Authorising Officer may stipulate a shorter period. This will be influenced by the sensitivity of the operation, particularly when there are concerns around the level of collateral intrusion, necessity, proportionality and the acquisition of confidential material.

Note: The current version of the **CS096A** is dual purpose and is also used to apply for an existing authorisation to be cancelled (see 5.4 below).

5.3 **Renewal of Authority** (Code of Practice Section 4.23- 4.27 refers)
As detailed at 3.10 above, a written authorisation granted by an Authorising Officer 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. Hence a written authority granted on the 24th April will cease at 23:59 hours on the 23rd July. If a renewal is authorised, this will taken effect at 00:00 hours on 24th July.

The Authorising Officer will stipulate the date on which a completed form **CS096** must be submitted. This is normally 6 days prior to the due cancellation date.

5.4 **Cancellation of Authority (Code of Practice Section 4.28-4.29 refers)**
Once the directed surveillance no longer meets the criteria upon which it was authorised i.e. suspect apprehended or no longer has access, all surveillance activity **must** cease.

In such circumstances and to protect the human rights of those who have been the subject of the surveillance, either directly or indirectly it is vital that directed surveillances are immediately cancelled through the submission of a **CS096A** to an Authorising Officer.

When doing so applicants must be clear as to the material acquired or produced as a consequence of the surveillance and what they are proposing to do with it e.g. destroy it, make it available of another process (conduct/ tribunal) or store it and use it in the criminal process.

The Authorising Officer when cancelling the surveillance will advise the applicant on the handling and disposal of such material.

POL00104796

6. URGENT ORAL AUTHORITIES

6.1 It is recognised that urgent situations will arise whereby it is not possible to prepare and submit a written application to carry out directed surveillance. The definition of 'directed surveillance' at 3.3 above, takes account of – 'an immediate response to events or circumstances, which, by their very nature, could not have been foreseen'.

6.2 In such urgent cases, an Authorising Officer, may grant oral authority to carry out specific activities. Oral authority (unless renewed in writing on form **CS096**) will be cancelled after 72 hours from the time the authorisation was granted.

6.3 As soon as is possible, the applicant must prepare, and submit to the Authorising Officer, a form **CS095B** (Application for Urgent Oral Authority) detailing the authorised activity. There is no requirement to record the case history.

6.4 The Authorising Officer will then prepare a form **CS095C** explaining the reason/s for urgency. The Covert Surveillance – Code of Practice (Section 4.13 refers) determines that: -

"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."

6.5 **Note:** If as a result of the authority the operation is successfully resolved then a cancellation form **CS096A** must be completed and submitted to the Authorising Officer as soon as possible.

6.6 For surveillance to continue beyond 72 hours then authority for renewal must be sought using the form **CS096**. To effectively comply with the Surveillance Codes of Practice it is vital that the preceding **CS095C** has been filled in accurately and in full. If there is doubt about this, or if the subject and/or operation is likely to change significantly, then application for continued directed surveillance must be completed on a new **CS095**.

7. AUTHORITY FOR 3RD PARTIES TO CARRY OUT DIRECTED SURVEILLANCE FROM OR WITHIN RM/PO PREMISES

7.1 On occasions the Police or other Designated Public Authorities wish to carry out directed surveillance from, or within our premises, as part of a criminal investigation.

7.2 Before allowing directed surveillance to take place, the Investigator must be satisfied the Police or Designated Public Authority concerned, has obtained the proper authorisation. Details must then be recorded using side A of form **CS095A**. Guidelines can be found on side B of the form.

7.3 A copy of the completed form **CS095A** must be provided to the relevant Territorial Investigation Manager/ Head of Security who will record the details on form **CS097**. A further copy should be provided to the '3rd party' concerned for their records and disclosure purposes.

POL00104796

7.4 Investigators must ensure when 3rd parties perform surveillance on 'Business' premises that our Health and Safety requirements are complied with.

8. GENERAL

8.1 After authorisation, the Authorising Officer will send the original completed Directed Surveillance forms to Corporate Security, Intelligence Operations Manager, Royal Mail, Corporate Security, Floor 2a, Battersea DO, 202 Lavender Hill, LONDON, SW11 1AA where a copy of all applications will be retained for a period of 5 years. All original documentation shall be returned to the applicant concerned

8.2 The Intelligence Operations Manager will perform a 'Gatekeeper' role and be responsible for recording the details of all applications made and monitoring the compliance in relation to reviews, renewals and cancellations.

8.3 Any unauthorised surveillance activity identified by Territorial Investigation Managers, Casework Managers or the Criminal Law Team etc, must be reported to the Performance & Planning manager.

8.4 All completed Directed Surveillance forms are considered to be 'disclosable material' and will be made available to defence.

8.5 The Surveillance Codes of Practice should be available on request.