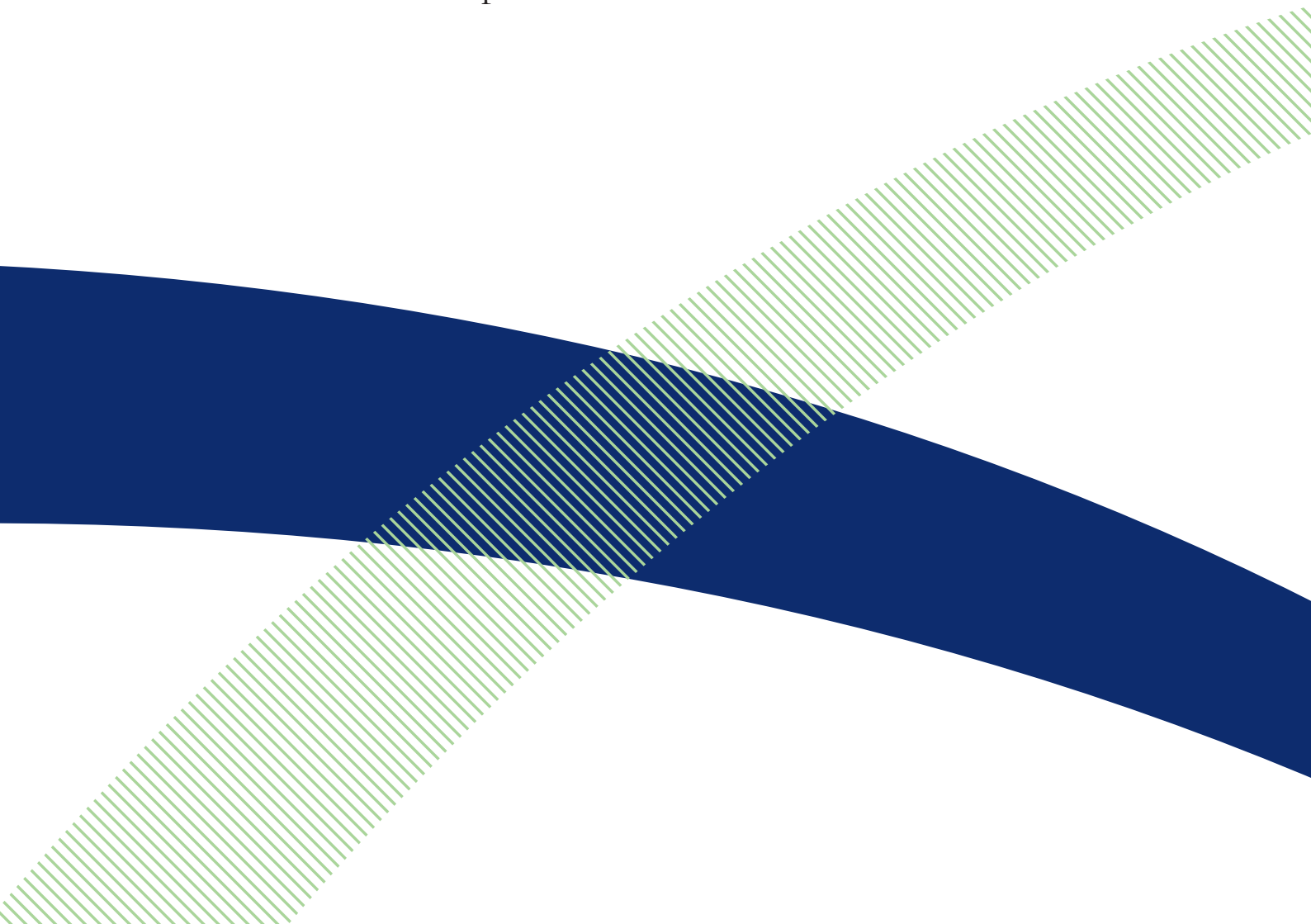
Home Office

REGULATION OF INVESTIGATORY POWERS ACT 2000:

Consolidating Orders and Codes of Practice

A Public Consultation Paper



Contents

Foreword

The Rt Hon Jacqui Smith MP, Home Secretary

Our country has a proud tradition of defending individual freedom – by protecting people's freedom from those who would do us harm and by safeguarding individuals' privacy from unjustified interference by the State. The Government is responsible for protecting both types of freedom. In order to do this, we must ensure that the police and other public authorities have the powers they need to carry out their functions. But we must also ensure that those powers are not used inappropriately.

The Regulation of Investigatory Powers Act 2000 ('RIPA') is central to protecting both types of freedom. Although it does not provide any new covert powers, it does ensure that public authorities which have a demonstrable need to use key investigatory techniques can do so – in order to protect our freedom from interference by those who would harm us. But it also ensures that those public authorities pay due regard to our right to privacy – so we can be free from unjustified interference by the State.

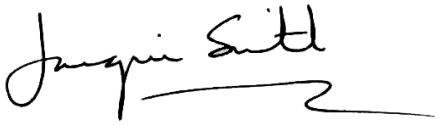
A wide range of public authorities use investigatory techniques under RIPA and they fulfil a range of functions. At one end of the spectrum, for example, those responsible for ensuring that taxpayers' money is not abused by benefit cheats can use surveillance under RIPA to follow and film someone in public places. They might do that if the person has claimed disability benefits for many years on the basis that he cannot walk long distances, but he actually spends his free time competing in marathons – as has actually happened. In my view, this is entirely appropriate. It's just common sense.

At the other end of the spectrum, a far smaller number of public authorities, such as the police and the Security Service, are able to use intrusive surveillance techniques, such as watching or listening to people in private places. They use these techniques to tackle more serious crimes, such as organised drugs trafficking, child abuse or terrorism. Again, it's just common sense that they should be able to do this – and I believe the public expects us to make sure the law enforcement agencies have the tools they need to keep us safe.

But I share concerns about how a small number of local authorities have used techniques under RIPA when most of us would say it was not necessary or proportionate for them to do so. As I have made clear, I do not think it is right for RIPA to be used to investigate offences relating to dog-fouling or to see whether people put their bins out a day early. This, too, is just common sense.

This consultation will help us ensure that investigatory techniques can continue to be used when they are necessary and proportionate, but that there is no repetition of the small number of cases when they have been misused. By raising the seniority of those who can authorise techniques under RIPA, and increasing the oversight, in local authorities, our proposals will help us get the balance right between supporting law enforcement and respecting privacy. They will provide clarity and transparency on which public authorities use which covert techniques, and the reasons they do so.

I would urge anyone with an interest in this matter to respond to this consultation.



Jacqui Smith MP

1. Executive Summary

For many years, public authorities, including the law enforcement and intelligence agencies, various regulatory bodies, and local authorities, have used a wide range of covert investigatory techniques. They use these techniques to investigate suspects without alerting them to the fact that they are under investigation.

Until 2000, when the Human Rights Act 1998 came into force and the Government passed the Regulation of Investigatory Powers Act 2000 (RIPA), public authorities could use most of these techniques free from statutory control[1]. They were not always required to consider whether it would be necessary and proportionate to use the techniques. They did not always have to justify the likely intrusion into the privacy of those under investigation – or even the privacy of others who could be affected. They were not required to authorise all the techniques at appropriately senior levels. They were not, in many cases, subject to independent oversight. There was no independent complaints mechanism. In short, the use of covert investigatory techniques by public authorities was largely unregulated.

RIPA addressed this situation. It is not anti-terrorism legislation. It did not create any covert powers. It did not give public authorities access to covert investigatory techniques for the first time. Rather, it created a regulatory framework to govern the way public authorities use these techniques.

Under RIPA, the most deeply intrusive techniques, such as intercepting communications or eavesdropping in private places, can only be used by a very limited set of public authorities[2]. And regardless of which technique is involved, if public authorities want to use any of them under RIPA, they must first be satisfied that it would be necessary and proportionate to do so. They must consider the impact of these techniques on the privacy of those under investigation, and on any other people who might be affected. Different techniques can only be used if they are authorised at appropriately senior levels; and the most deeply intrusive techniques are subject to prior independent approval. Public authorities using techniques under RIPA are now subject to independent inspection. Finally, there is an independent tribunal, the Investigatory Powers Tribunal, to consider any complaints relating to the way investigatory techniques regulated by RIPA have been used.

RIPA and its associated Codes of Practice have, therefore, greatly improved control and oversight of the way public authorities use key investigatory techniques, in order to protect our right to privacy.

The Government recognises, however, that public authority use of these investigatory techniques must be kept under review. In particular, there have been a number of occasions recently when public authorities have used techniques under RIPA when most people would have regarded it as inappropriate to do so. The Government is committed to ensuring that these examples are not repeated. This consultation will help achieve this.

This consultation includes details about all the public authorities able to use certain techniques under RIPA, including the ranks at which those techniques can be authorised and the purposes for which they can be used. This is so that members of the public can consider whether it is appropriate for these public authorities to be part of the RIPA framework. It will also allow the Government to revise the ranks at which RIPA techniques can be authorised.

In light of recent public concerns, the Government is particularly interested in proposals concerning the way local authorities use techniques under RIPA. The Government is clear that techniques authorised under RIPA should not be used for trivial purposes, such as investigating dog-fouling offences. In order to ensure local authorities only use techniques under RIPA when it is appropriate to do so, the Government is proposing raising the rank at which RIPA authorisations can be granted within local authorities to senior executives. It is also considering creating a role for elected councillors in overseeing the way in which local authorities use RIPA techniques.

1 The use of interception was governed by the Interception of Communications Act 1985 and the use of property interference by a limited number of public authorities was governed by the Police Act 1997 and the Intelligence Services Act 1994.

2 See sections 6, 32 and 41 RIPA, and chapter 8, below.

This consultation also includes related draft Codes of Practice. These would replace the existing Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources. They are intended to provide greater clarity on when the use of RIPA techniques is likely to be proportionate. They reflect proposals to ensure that surveillance of legally privileged communications or communications between constituents and MPs on constituency business is subject to proper safeguards. The proposals relating to legally privileged communications reflect separate draft statutory instruments which the Home Secretary intends to publish shortly, in light of a House of Lords judgment received in March[3]. The draft Codes of Practice are also designed to reduce bureaucracy, following Sir Ronnie Flanagan's Review of Policing, by clarifying when public authorities do not need to use RIPA authorisations and by facilitating the work of police collaborative units (together with proposals in the Policing and Crime Bill currently before Parliament). Together, these changes will help free up police time so they can get on with the job that the public expect them to do, catching criminals.

The Government is asking:

1. Taking into account the reasons for requiring the use of covert investigatory techniques under RIPA set out for each public authority, should any of them nevertheless be removed from the RIPA framework?
2. If any public authorities should be removed from the RIPA framework, what, if any, alternative tools should they be given to enable them to do their jobs?
3. What more should we do to reduce bureaucracy for the police so they can use RIPA more easily to protect the public against criminals?
4. Should the rank at which local authorities authorise the use of covert investigatory techniques be raised to senior executive?
5. Should elected councillors be given a role in overseeing the way local authorities use covert investigatory techniques?
6. Are the Government's other proposed changes in the Consolidating Orders appropriate?
7. Do the revised Codes of Practice provide sufficient clarity on when it is necessary and proportionate to use techniques regulated in RIPA?

3 In re McE (Appellant) (Northern Ireland), In re C (AP) and another (Appellants) (Northern Ireland), In re M (Appellant) (Northern Ireland) [2009] UKHL 15. See chapter 4 in the draft Codes of Practice on Covert Surveillance and Property Interference, and Covert Human Intelligence Sources, below.

2. Introductory Q & A

What are covert investigatory techniques?

Covert investigatory techniques are ways of investigating someone without alerting them to the fact that they are under investigation. The key techniques addressed in this consultation are covert surveillance – that is, monitoring someone without them knowing – and the use of covert human intelligence sources (CHIS) – that is, people who use a relationship for the covert purpose of obtaining information. Specified public authorities are also able to access certain information about communications. This can be done covertly, for instance if it is part of an ongoing investigation, or overtly, for example in order to assist a coroner's inquest. Further details about all these techniques are provided below.

Why do public authorities use covert investigatory techniques?

It may be necessary to prevent a person realising that they are under investigation. If this could not happen, criminals and other people who threaten our well-being would often be able to get away with their crimes or wrongdoings.

What is the Regulation of Investigatory Powers Act 2000 (RIPA)?

RIPA regulates the way in public authorities use a range of investigatory techniques. It is not anti-terrorist legislation. It did not create any new covert powers. Rather, it provides a framework within which key investigatory techniques can be used compatibly with the European Convention on Human Rights, and particularly our right to privacy.

How does RIPA relate to the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A)?

RIP(S)A performs the same role as RIPA, but in relation to devolved matters, that is, matters over which the Scottish Government has jurisdiction. These include crime, but not national security or the economic well-being of the UK. RIP(S)A is not directly relevant to this consultation.

What does this consultation cover?

This consultation covers 'Consolidating Orders' which list the public authorities able to use a number of covert investigatory techniques under RIPA. It also covers related draft Codes of Practice. The techniques are explained below.

How does this relate to the Communications Data Consultation?

This consultation is about how covert techniques are currently authorised and governed under RIPA, including which public authorities may seek access to specific communications data and how they may do so. The Communications Data consultation is about maintaining our communications data capability in the future, in light of changing communications technology. It does not cover public authority access to and use of communications data. It will be published shortly.

How does this relate to the European Data Retention Directive?

The Data Retention Directive, implemented recently through the Data Retention (EC Directive) Regulations 2009, requires public communications service providers to retain communications data which they process or generate in the course of their business. As far as communications data is concerned, RIPA governs how public authorities can access it, and how that access is overseen.

Which public authorities are covered in this consultation?

The key public authorities identified in RIPA are the law enforcement and intelligence agencies. These need to use the full range of covert investigatory techniques on a regular basis in order to do their job.

Other public authorities are identified in Schedule 1 to RIPA and/or have been added to the RIPA framework by statutory instrument. These include local authorities and regulatory bodies. The use of investigatory techniques by these public authorities is more limited. Their need to do this can be important, but, unlike the police and intelligence agencies, use by these bodies is relatively infrequent.

What do the Consolidating Orders do?

The draft Consolidating Orders orders list all the public authorities able to grant authorisations under RIPA in respect of:

1. Directed surveillance (covertly monitoring the movements and actions of specifically targeted individuals in public places);
2. Covert human intelligence sources (people who at the direction of a public authority establish or maintain a relationship with someone else for the covert purpose of obtaining and disclosing information);
3. Communications data (the who, where and when of a communication, but not the content).

The Consolidating Orders list the public authorities which can use these techniques under RIPA, the purposes for which they can use the techniques and the ranks at which the techniques can be authorised.

They do not cover:

I. Intrusive surveillance (covert surveillance in residential premises or in a private vehicle);

II. Interception of communications (making the contents of a communication available during the course of its transmission to a person other than the sender or intended recipient).

These techniques are restricted to key public authorities such as the police and the security and intelligence agencies as specified in the Act[4]. Most public authorities, such as local authorities, are not able to use these techniques.

What is the Government proposing to change in the Consolidating Orders?

There are good reasons for local authorities to be able to use some basic covert techniques regulated by RIPA. Local authorities do very important work to tackle, for example, fraud and trading standards issues.

Case study – local authority use of covert techniques regulated in RIPA

A local authority's Trading Standards Unit used directed surveillance and communications data authorised under RIPA to prosecute three roofers who had persuaded 11 elderly victims to pay for unnecessary work on their roofs. The victims lost in excess of £150,000. Two of the 11 victims lost their entire life savings (£79,000 and £58,500). The three criminals responsible were sentenced to between 3 and 6 years imprisonment.

But the Government is not satisfied that local authorities have always applied consistent standards in deciding whether to authorise techniques under RIPA. The Government proposes to address this partly through the revised Codes of Practice, discussed below. But it is also considering raising the rank at which techniques are authorised in local authorities to senior executive, and giving elected councillors a role in overseeing the way RIPA techniques are used. Subject to the outcome of this consultation exercise, this would be done primarily through the Consolidating Orders.

The Government is proposing to make a number of other minor changes. These reflect organisational and name changes and, in some instances, reflect changes in capability that mean certain public authorities no

4 See sections 6, 32 and 41 RIPA, and chapter 8 below.

longer require the ability to use certain covert techniques. These changes are all identified in the Consolidating Orders table in bold font.

What do the Codes of Practice do?

The Codes of Practice provide statutory guidance on when and how covert investigative techniques should be authorised, the circumstances in which they should be used, and how they are reviewed and overseen by independent Commissioners. The revised Codes of Practice have been drafted in consultation with practitioners and other stakeholders. They are intended to provide greater clarity on when certain techniques should or should not be used, including by local authorities. They will:

- ensure that the tests of necessity and proportionality are better understood and applied lawfully, consistently and with common sense;
- require constituents' communications with their MPs on constituency business to be treated in the same way as other confidential material, following the report of Sir Christopher Rose into the bugging of conversations between Babar Ahmad and Sadiq Khan MP;
- reduce bureaucracy for the police and other public authorities by providing greater clarity on when authorisations are not needed and by supporting proposals in the Policing and Crime Bill to facilitate the work of police collaborative units, in line with a recommendation in Sir Ronnie Flanagan's Review of Policing;
- make further, minor changes to reflect recent legal and operational developments.

We are publishing two draft Codes of Practice for consultation. The draft Code of Practice on Covert Surveillance and Property Interference covers:

1. directed surveillance (this is relevant to all public authorities specified in Schedule 1, RIPA);
2. intrusive surveillance; and,
3. property interference and wireless telegraphy (entering onto or interfering with property or with wireless telegraphy, for example entering premises covertly in order to facilitate surveillance).

Intrusive surveillance and property interference are restricted to key public authorities such as the police and the security and intelligence agencies as specified in the Act[5]. No other public authorities, including all local authorities, can use intrusive surveillance or interfere with property under RIPA.

The draft Code of Practice on Covert Human Intelligence Sources covers the authorisation by public authorities of the conduct or use of individuals who establish or maintain a relationship with someone else for the covert purpose of acquiring information and passing it on to a relevant public authority. This is relevant to all public authorities specified in Part 1 of Schedule 1, RIPA.

What about the Codes of Practice on Communications Data and Interception?

A Code of Practice on the Acquisition and Disclosure of Communications Data was issued in 2007 after public consultation. There is no requirement for further revision.

The Government is proposing to make a small number of changes to the Interception Code of Practice. As warranted interception can only be carried out by a restricted set of key public authorities, primarily the law enforcement and intelligence agencies,[6] and as the changes to the code are minor, the Government is not including the revised interception code in this consultation exercise. The revised code will, however, be

5 See sections 6, 32 and 41 RIPA, and chapter 8 below. Property interference by the intelligence agencies is authorised under the Intelligence Services Act 1994.

6 Interception can also be carried out in penal establishments under prison rules, or for lawful business purposes under business practice regulations. In both these circumstances, those people whose communications may be intercepted are informed in advance that this may happen.

published (and any representations made on the code will be considered) before being subject to debate in Parliament and replacing the existing code.

What else has the Government done to help public authorities, such as the police, use covert techniques efficiently?

The Government has worked with a range of key partners, including the police and the National Police Improvement Agency, to reduce the number of occasions when RIPA authorisations are sought when they are not necessary. This work has already been successful. For example, the total number of authorisations for directed surveillance by law enforcement agencies, primarily the police, fell from 26,986 in 2003/04 to 18,767 in 2007/08[7].

When would the police and other public authorities not need to seek a RIPA authorisation?

The police and other public authorities do not need to seek a RIPA authorisation just because they are going to use covert techniques. A RIPA authorisation is only needed when the techniques are likely to result in the acquisition of information relating to a person's private or family life. This means that the police would not normally need a RIPA authorisation if they wanted to, for example, deploy plain clothes police officers on patrol in a town centre to see if offences such as shoplifting take place, or review CCTV footage in order to reconstruct the circumstances in which a crime was committed.

Why is the Government launching this consultation now?

The Government is clear that the use of covert investigatory techniques to deliver public safety must command public confidence and must take place in accordance with the law and with respect for individuals' rights. This consultation will ensure that there is full transparency about which public authorities can use different techniques, and the circumstances in which those techniques can be deployed. In view of recent public concern, the Government is seeking views on possible changes to the way in which local authorities authorise and use techniques regulated in RIPA.

What is the Government asking in this consultation exercise?

The Government is asking:

1. Taking into account the reasons for requiring the use of covert investigatory techniques under RIPA set out for each public authority, should any of them nevertheless be removed from the RIPA framework?
2. If any public authorities should be removed from the RIPA framework, what, if any, alternative tools should they be given to enable them to do their jobs?
3. What more should we do to reduce bureaucracy for the police so they can use RIPA more easily to protect the public against criminals?
4. Should the rank at which local authorities authorise the use of covert investigatory techniques be raised to senior executive?
5. Should elected councillors be given a role in overseeing the way local authorities use covert investigatory techniques?
6. Are the Government's other proposed changes in the Consolidating Orders appropriate?

7 See the Annual Reports of the Chief Surveillance Commissioner for 2003/04 and 2007/08. The Report for 2007/08 also notes that, in relation to other public authorities, directed surveillance authorisations fell from 12, 494 the previous year to 9, 535 in 2007/08. The Chief Surveillance Commissioner noted that this represented a significant decrease; although it is still a net increase from 2003/04 when 6, 398 authorisations were granted.

7. Do the Codes of Practice provide sufficient clarity on when it is necessary and proportionate to use techniques regulated in RIPA?

What will happen next?

After this consultation exercise, the Government will bring forward statutory instruments to give effect to the Codes of Practice and the Consolidating Orders. These will be debated in Parliament.

3. The Techniques Covered in the Consultation

The Consolidating Orders list the public authorities able to use:

- communications data;
- directed surveillance; and,
- covert human intelligence sources.

The revised Codes of Practice cover:

- covert surveillance and property interference; and
- covert human intelligence sources.

A statutory Code of Practice on the Acquisition and Disclosure of Communications Data came into effect in October 2007.

3.1 Communications Data

Communications data is information about a communication. It does not include the content of a communication. It can show when a communication happened, where it came from and where it was going, but it cannot show what was said or written.

For a given telephone call, communications data can include the telephone numbers involved, and the time and place the call was made, but not what was said. For an e-mail it might include the e-mail address from which the message was sent, and where it was sent to, but not the content of the e-mail.

When used by law enforcement agencies, communications data plays a key role especially in the fight against terrorism and the prosecution of serious crimes such as child sex abuse, kidnap and murder. It has been used in almost all Security Service operations since 2004. When used by other agencies it provides vital intelligence, and evidence to prosecute, in investigations into other crimes, to protect from injury in areas such as public health and safety, and to safeguard life in the case of the work of the emergency services.

Under the Data Retention (EC Directive) Regulations 2009, public communications service providers issued with a notice by the Secretary of State must retain their communications data for 12 months. This is consistent with the requirements of European Directive 2006/24/EC. This would also be in line with provisions agreed by Parliament for the voluntary retention of communications data under Part II of the Anti-Terrorism Crime and Security Act 2001. Data required in connection with legal processes (for example to provide evidence in a criminal trial) may be retained for longer periods. In addition to being accessible under RIPA, communications data can be accessed in limited circumstances through other methods, such as a court order issued under the Police and Criminal Evidence Act 1984 or section 1 of the Social Security Fraud Act 2001.

Three different types of communications data are specified in RIPA:

Traffic data

This includes information on where the equipment used in the communication was located when the communication took place (for example, the location of the mobile phone from which a text message was sent and the location of the mobile phone which received it). This type of communications data is the most intrusive. Its use is limited to those public authorities which have shown that they require it to fulfil their statutory functions (such as the emergency services and law enforcement, security and intelligence agencies). Other public authorities, which do not have such a need, cannot obtain this type of data under RIPA. Local authorities do not have access to traffic data.

Service use

This includes information retained by the service provider about the use made by a person of the service concerned. For example, how the communication occurred (for instance, a telephone call, text message or e-mail), when the communication happened (the date and time of the call) and how long it lasted. These sorts of data are very often required by the service provider for billing purposes and make up the information listed on the itemised invoice sent to the subscriber. All listed public authorities may request access to specified service use data.

Subscriber data

This is the information subscribers give to the service provider when they sign up to a communications service. It includes personal details such as the subscriber's name and address and any direct debit details provided at the time of subscription. All listed public authorities may request access to specific subscriber data.

Case study – traffic and service use data

During 2006-07, a gang carried out a series of armed robberies in southern England. These ended when police shot dead two gang members. The gang stole £500,000 by robbing security vans making deliveries to banks. Mobile phone records, including traffic data, were used to show that they had been at the scenes of a series of raids exactly a week before the crimes. Their phones were then all turned off for the duration of the robberies. Service data showed that they had all been in contact with the individual who had been the gang's recruiter. Two of the gang members, Terence Wallance and Adrian Johnson, were given prison sentences of 17 years. Five other gang members received sentences ranging from 5 to 12 years.

Case study – service use and subscriber data

Birmingham City Council has used service use and subscriber data, as well as directed surveillance, in illegal money lending investigations. In one case, a violent loan shark, Kim Cornfield, lent small amounts of cash, but charged extortionate interest rates, including one of 15,000%. He used threats of violence and physical abuse to enforce payment. He demanded 'payment in kind' from women who were not able to repay him. While subject to an injunction, he used his mobile phone to text victims to threaten them with violence if they gave evidence against him. Service use and subscriber data demonstrated that he had sent the text messages received by the victims. Faced with the evidence against him, he pleaded guilty to blackmail and illegal money lending. He was sentenced to two years in prison in February 2006.

3.2 Directed And Intrusive Surveillance

Directed surveillance

'Directed' surveillance is covert surveillance by public authorities in public places for the purposes of a specific investigation or operation which is likely to obtain private information about a person and which is undertaken otherwise than as an immediate response to events or circumstances. This can include the covert use of:

- observation of movements;
- eavesdropping on conversations;
- photographing or filming; and
- tracking vehicles either in person or with the use of cameras or recording devices.

Case study – directed surveillance

In 2005, officers from the Department of Work and Pensions (DWP) investigated an individual, Paul Appleby, who had claimed over £22,000 in disability benefits over several years. He alleged that he was unable to walk long distances and needed help with feeding and other activities. DWP investigators filmed him during 2005 warming up for races and running with his local athletics club. They were also able to establish that he had taken part in several marathons. He admitted failing to notify the DWP of a change in his circumstances and was given a ten month custodial sentence.

Intrusive surveillance

'Intrusive' surveillance is covert surveillance in private places such as people's houses or cars. It is regulated separately in RIPA, available only to key public authorities such as the police and security and intelligence agencies, and subject to more stringent authorisation requirements. Intrusive surveillance cannot be used by the majority of public authorities listed in the Consolidating Orders, including local authorities. It is necessary, however, to set out the guidance for its use, and the associated requirement for property interference in the revised Code of Practice on Covert Surveillance and Property Interference.

Case study – intrusive surveillance

On 18 February 2008, Parviz Khan, a British national of Pakistani origin, was sentenced to life imprisonment for his role in planning to abduct and murder a British Muslim soldier for extremist propaganda purposes. Much of the evidence used in the case against Khan derived from eavesdropping coverage of his conversations, which was obtained under the authorisation of a property and intrusive surveillance warrant obtained from the Secretary of State by the Security Service.

Case study – intrusive surveillance

West Midlands police force carried out an investigation into a murder after a body was found. The investigation initially suggested that the victim's former partner was responsible. Intrusive surveillance was deployed to listen to the suspect's conversations in private. This was able to establish that the suspect was not responsible and provided valuable information allowing the police to pursue a different line of inquiry.

3.3 Covert Human Intelligence Sources

A covert human intelligence source (CHIS) is someone authorised by a public authority to establish or maintain a relationship, in order covertly to obtain information and disclose it to the relevant public authority. The person acting as a covert human intelligence source can be an undercover officer or a tasked informant.

Case study – covert human intelligence sources

The Food Standards Agency deployed a CHIS to obtain detailed information on an approved slaughterhouse they suspected of being run by someone subject to a prohibition order under the Food Safety Act 1990. Illegal meat production means that the meat has not necessarily undergone proper veterinary inspection or been health marked as fit for human consumption (a requirement for placing it on the market). It also raises grave bio-security concerns as there is unlikely to be any control on the storage and disposal of animal by-products. This could result in the spread of animal diseases such as avian influenza and foot and mouth disease. In this case the evidence obtained by the CHIS enabled the subject to be convicted and given a suspended prison sentence and a community service order.

4. RIPA Safeguards

The techniques regulated in RIPA are subject to stringent safeguards approved by Parliament to ensure that investigatory powers are exercised compatibly with the ECHR. In particular, the substantive protections of Article 8 (right to respect for private and family life) are guaranteed by the express terms of RIPA which only permit the authorisation of the relevant techniques if the tests of necessity and proportionality are satisfied.

4.1 Necessary Purpose Limitation

Covert investigatory techniques can only be authorised under RIPA when their use would be necessary on specified grounds. In the case of communications data (section 22), directed surveillance (section 28) and covert human intelligence sources (section 29) the specified grounds are:

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or preventing disorder;

(c) in the interests of the economic well-being of the UK;

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other charge payable to a Government Department.

RIPA provides an extra purpose for communications data only:

(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

Further grounds can be specified by an Order made by the Secretary of State (sections 22(h) (communications data), 28(g) (directed surveillance) and 29(g) (covert human intelligence sources)).

SI No.1878 of 2006 provides the following additional grounds in relation to communications data:

- Article 2(a) - to assist investigations into alleged miscarriages of justice; and
- Article 2(b) - to assist in identifying a person who has died or is unable to identify himself because of a physical or mental condition, other than one resulting from crime, or to obtain information about his next of kin or others connected with him or about the reason for his death or condition.

4.2 Proportionality

The use of techniques regulated in RIPA can only be authorised if the conduct in question is proportionate to what is sought to be achieved by carrying it out. For example, the technique cannot be used if the information sought could reasonably be obtained by other, less intrusive means. When considering whether the use of a technique would be proportionate, authorising officers must therefore consider both the benefits to the investigation and the seriousness of the offence being investigated.

4.3 Authorisation Levels And Process

The use of covert techniques under RIPA can only be authorised by designated officers of sufficient seniority of rank or grade within each public authority. In the case of the most intrusive techniques, independent prior approval is required. Authorising officers, and those who give independent prior approval, must have the necessary level of oversight, judgement and objectivity to validate applications. They must also have sufficient

understanding of operational realities to give them a clear knowledge of what is reasonable and workable.

There is a different authorisation process for each covert technique.

- **Directed surveillance** and **covert human intelligence sources** are authorised internally, where the appropriate tests are met, by the senior officer designated in the relevant public authority. They are subject to oversight and inspection by the relevant oversight Commissioner (see below). The information to be provided to the authorising officer is set out in the relevant Code of Practice, and must be retained for future inspection. Authorisations are subject to regular reviews.
- **Intrusive surveillance** by the police and law enforcement agencies can only be authorised by the relevant Chief Officers or a designated deputy and requires prior independent approval by a Surveillance Commissioner. Intrusive surveillance by the intelligence agencies requires prior independent approval by the Secretary of State.
- **Property interference** by the police and law enforcement agencies requires prior authorisation by the relevant Chief Officer or a designated deputy and requires prior independent approval by a Surveillance Commissioner if it involves entry to residential or office premises or is likely to result in the acquisition of knowledge relating to legal privilege, confidential personal information or confidential journalistic information. Property interference by the intelligence services requires prior independent approval by the Secretary of State.
- **Communications data** is authorised through a distinct procedure. First, the officer seeking to access communications data completes an application form which must contain specific information as set out in the statutory Code of Practice. A 'single point of contact[8] then considers whether the application is lawful and whether it is feasible to obtain the specific communications data requested. A 'designated person' – a senior officer in the same public authority (as listed by Orders) – then considers whether the case is necessary and proportionate. A 'senior responsible officer' in the organisation is responsible for ensuring the authorisation process is lawful and that relevant records are maintained for inspection by the oversight Commissioner (see below).

4.4 Oversight

There are three independent Commissioners who have all held high judicial office and are responsible for providing oversight of different aspects of RIPA.

The Interception Commissioner, Sir Paul Kennedy, is responsible for overseeing of public authority use of interception and communications data under section 57 RIPA.

The Chief Surveillance Commissioner, Sir Christopher Rose, is responsible for overseeing the way in which public authorities (apart from the intelligence agencies) use covert surveillance and covert human intelligence sources, under section 62 RIPA.

The Intelligence Services Commissioner, Sir Peter Gibson, oversees the use of covert surveillance and covert human intelligence sources by the intelligence agencies, under section 59 RIPA.

4.5 Guidance

RIPA requires the Secretary of State to issue statutory Codes of Practice relating to the exercise and performance of the powers and duties conferred by RIPA. These codes help practitioners assess whether and in what circumstances covert techniques are appropriate, and give guidance on the procedures to be followed in each case. The Codes of Practice must be approved and debated in both House of Parliament and published. Any person exercising or performing any power or duty under RIPA must have regard to the provisions of the

8 A single point of contact ('SPOC') is a qualified designated intermediary who liaises between the a public authority seeking communications data and the relevant communications service provider.

relevant Code of Practice and the Code may be taken into account by the Courts, the Investigatory Powers Tribunal or the Commissioners.

The Government is revising the Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources. It has published draft Codes as part of this consultation.

The current versions of the Codes, including the Code on the Acquisition and Disclosure of Communications Data which came into effect in October 2007, are available on the Home Office website:

Access to Communications Data – copy available at:
http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/acquisition-disclosure-cop.pdf?view=Binary

Covert Surveillance – copy available at:
http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/covert-cop?view=Binary

Covert Human Intelligence Sources – copy available at:
http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/human-cop?view=Binary

4.6 Independent Complaints Mechanism

An Investigatory Powers Tribunal (IPT) established under section 65 of RIPA investigates complaints made by people who are concerned that public authorities have deployed covert investigatory techniques against them unlawfully. The Tribunal is independent of Government and currently consists of seven senior members of the legal profession in the UK appointed by Her Majesty. Both the President and Vice President of the Tribunal must hold or have held high judicial office. If the IPT determines the complaint in favour of the complainant, it is required to notify the complainant. It may, if appropriate, quash any authorisation, order the destruction of relevant material, award compensation or make any other order as it sees fit.

Information on the outcome of its adjudications is not made public, but information on the numbers of the cases it deals with is included in both the Interception of Communications Commissioner's and the Intelligence Services Commissioner's reports which are published annually. Confidentiality restrictions in RIPA preclude disclosure by the IPT of information to any third party in order to retain public confidence in its work. People would be deterred from making a complaint if they knew the Tribunal could not assure them appropriate confidentiality. There is no domestic right of appeal against IPT decisions, although individuals may seek appeal to the European Court of Human Rights.

The IPT's website is at:
http://www.ipt-uk.com/.

5. Consultation Questions

5.1 Your comments and views are invited on the following questions:

1. Taking into account the reasons for requiring the use of covert investigatory techniques under RIPA set out for each public authority, should any of them nevertheless be removed from the RIPA framework?
2. If any public authorities should be removed from the RIPA framework, what, if any, alternative tools should they be given to enable them to do their jobs?
3. What more should we do to reduce bureaucracy for the police so they can use RIPA more easily to protect the public against criminals?
4. Should the rank at which local authorities authorise the use of covert investigatory techniques be raised to senior executive?
5. Should elected councillors be given a role in overseeing the way local authorities use covert investigatory techniques?
6. Are the Government's other proposed changes in the Consolidating Orders appropriate?
7. Do the Codes of Practice provide sufficient clarity on when it is necessary and proportionate to use techniques regulated in RIPA?

6. How to respond to the Consultation

Please send responses to this consultation by 10 July 2009:

- **by e-mail to** RIPACONSULTATION@homeoffice.gsi.gov.uk; or
- **by post to** Tony Cooper, Home Office, 5th Floor Peel Building, 2 Marsham Street, London SW1P 4DF.

6.1 Alternative Formats

Should you require a copy of this consultation paper in any other format (for instance Braille, large font or audio) please contact Tony Cooper at the address above.

6.2 Responses: Confidentiality and Disclaimer

The information you send us may be passed to colleagues within the Home Office, the Government or related agencies.

It is intended to publish a summary of the responses to this Consultation on the Home Office website. Information provided in response to this Consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000, the Data Protection Act 1998 and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please be aware that, under the Freedom of Information Act, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this, it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

Please ensure that your response is marked clearly if you wish your comments and name to be kept confidential. Confidential responses will be included in any statistical summary of numbers of comments received and views expressed. The Department will process your personal data in accordance with the Data Protection Act. In the majority of circumstances this will mean that your personal data will not be disclosed to third parties.

This consultation follows the Government's Code of Practice on Consultation, the criteria for which are set out in Annex B.

HOME OFFICE

April 2009

7. Consolidating Orders Table

7.1 Public Authorities listed under RIPA

A. Public authorities able to carry out intrusive surveillance

Police

- uphold the law, prevent crime, bring to justice those who break the law

Transport Police

- polices national rail network, London Underground & Eurostar

Armed Service Police

- counters hostile surveillance and other support to UK armed services

MOD Police

- guards Britain's nuclear deterrent and other high security defence sites

SOCA

- intelligence-led law enforcement agency, tackling trafficking, counterfeiting, hi-tech crime and child protection

HMRC

- polices system of revenue/taxes/duties and provides frontier protection against smuggling

Security Service

- protects UK from threats to national security

SIS

- collects UK's foreign intelligence

GCHQ

- protects Government communications and information systems from compromise

Armed Services

- conducts military operations to defend UK and Overseas Territories

Ministry of Defence

- combats crime or disorder affecting the armed services

Office of Fair Trading

- combats breaches of competition law (such as cartels) and consumer crime (such as bogus lotteries and competitions) on a national scale

B. Public authorities listed in the Schedule to RIPA or added by Statutory Instrument

Ambulance Services

- emergency 999 service (also provides details to police on assaults on staff, inappropriate and hoax 999 calls)

Charity Commission

- investigates charities fraud, including money laundering and links with proscribed organisations

Child Maintenance and Enforcement Commission

- calculates, collects and enforces child maintenance liabilities from absent partners

Care Quality Commission (formerly the Commission for Healthcare Audit & Inspection)

- inspects dangerous NHS and other health service premises and practices and enforces breaches in health care law (eg MRSA)

Civil Nuclear Constabulary

- protects designated civil nuclear sites and nuclear materials in transit

Criminal Cases Review Commission / Scottish CCRC

- investigates potential miscarriages of justice

Department of Agriculture and Rural Development in NI

- enforces range of animal health legislation, including enforcing BSE controls and combating subsidy & compensation fraud

Department for Business, Enterprise & Regulatory Reform

- combats anti-competitive business practices such as insolvency fraud, unscrupulous trading practices and breaches in employment legislation

Department of Enterprise, Trade and Investment For NI

- undertakes in NI functions by local council trading standards and the Health & Safety Executive in the rest of the UK

Department of Environment, Food and Rural Affairs

- Investigation Services combat areas such as trade in illegal veterinary medicines
- Marine & Fisheries Agency enforces sea fishing legislation (for instance relating to foreign fishing rights)
- Centre for Environment, Fisheries & Aquaculture Science enforces import regulations to prevent disease in freshwater fish/shellfish farms

Department of Health – Medicines & Healthcare Products Regulatory Agency

- prevents or takes out of circulation unlicensed, unlawful or counterfeit medicines and medical devices which can cause harm or loss to life

Department for Transport – Accident Investigation Branches

- determines the causes of accidents or incidents which may include loss of life to improve safety standards and prevent further occurrences

Department for Transport – Driving Standards Agency

- reduces deaths on the road by untested/unqualified drivers by combating fraudulent attacks on the driving test system

Department for Transport – Maritime and Coastguard Agency

- provides emergency lifeboat search and rescue and enforces breaches of maritime law relating to defective shipping and seaborne pollution

Department for Transport – Vehicle and Operator Services Agency

- enforces statutory safety measures for road vehicles (eg combating fraudulent MOT garages, unlicensed or overloaded goods vehicles)

Department for Work and Pensions

- investigates employment benefit fraud by individuals and organised criminals

Environment Agency / Scottish Environment Protection Agency

- combats environmental pollution, including from large-scale waste dumping and unregulated landfill on national scale

Financial Services Authority

- maintains financial market confidence by prosecuting illegal business practices such as insider dealing under the Criminal Justice Act 1993

Fire & Rescue Services

- provides emergency response to save lives and protect property, enforces fire safety regulations and investigates fire setting incidents

Food Standards Agency

- enforces slaughterhouse legislation to ensure unfit meat does not enter the human food chain and cause harm or death

Gambling Commission

- licenses all gambling to ensure the public are protected from cheating, intimidation and risks to vulnerable people such as children

Gangmasters Licensing Authority

- prevents the exploitation and possible death of migrant workers by unlicensed labour providers

Health and Safety Executive

- enforces work related health & safety legislation to prevent major risks to people (such as the December 2005 Buncefield oil depot explosions)

HM Chief Inspector Of Education, Children's Services & Skills

- enforces childcare legislation to ensure all children in regulated care are safe

Home Office - UK Border Agency

- combats immigration crime and asylum fraud and runs removal centres for people detained under immigration law

Independent Police Complaints Commission

- oversees the handling of public complaints of misconduct by police and other law enforcement agencies

Information Commissioner

- enforces access to official information and the protection of personal information, including attempts to contravene legal requirements

Local Authorities

- enforce law relating to such areas as trading standards and waste dumping and tackles housing benefit and council tax fraud

Ministry Of Justice

- responsible for holding prisoners securely and providing safe and well-ordered detention establishments

NHS Services

- counter fraud and corruption in the provision of NHS services which divert valuable resources away from front-line patient care

Northern Ireland Office – Prison Service

- responsible for holding prisoners securely and providing safe and well-ordered detention establishments

Office of Communications

- combats unlicensed broadcasters which pay no taxes, provide unfair competition, alienate audiences and interfere with 999 transmissions

Office of The Police Ombudsman For Northern Ireland

- oversees the handling of public complaints of misconduct by police and other law enforcement agencies in Northern Ireland

Pensions Regulator

- ensures company pension schemes are offered and managed fairly and legally and that funds are not transferred into bogus schemes

Ports Police (Dover and Liverpool)

- provides policing services within one square mile of the dock areas (eg crime associated with commercial and passenger services)

Postal Services Commission

- combats the operation of unlicensed mail services and people interfering with the mail in the course of its transmission

Royal Mail

- combats theft from the Royal Mail, Post Office and Parcelforce (incl. identity and financial information and stolen goods from the internet)

Royal Pharmaceutical Society of Great Britain

- protects the public by ensuring that controlled drugs, poisons and prescription medicines are managed and sold safely and legally

Scottish Crime and Drug Enforcement Agency

- disrupts and dismantles serious crime groups operating in Scotland, including by taking the profit out of crime

Serious Fraud Office

- combats serious or complex fraud where monies at risk are at least £1m, there is a national concern or specialist skills are needed

Welsh Assembly Government

- tackles breaches in health & social care (such as children's care), farming subsidies and sea fishing law (such as catch sizes)

7.2 Public Authorities able to carry out Intrusive Surveillance

NB. Significant proposed changes identified below in **bold.**

POLICE FORCES

- A police force maintained under s2 of the Police Act 1996
- The Metropolitan Police Force
- The City of London Police Force
- The British Transport Police
- A police force maintained under or by virtue of s1 of the Police (Scotland) Act 1967
- The Police Service of Northern Ireland

Responsible for upholding the law, preventing crime, pursuing and bringing to justice those who break the law, keeping the Queen's peace and protecting, assisting and reassuring members of the public.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Superintendent	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (a) national security (b) preventing or detecting crime or disorder (c) economic well being of UK (d) public safety (e) public health (g) in an emergency preventing death/ injury Article 2(b) identifying person
Inspector	RIPA S21(4) (c) subscriber data	
Superintendent Inspector England/Wales/Scotland - Chief Constable Metropolitan Police - Assistant Commissioner City of London Police - Commissioner PSNI – Deputy Chief Constable England/Wales/Scotland - Assistant Chief Constable Metropolitan Police - Commander City of London Police – Commander PSNI – Assistant Chief Constable	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases Where Confidential information is likely to be obtained When a vulnerable person/juvenile is to be used as a CHIS	RIPA S28(3) & S29(3) (a) national security (b) preventing or detecting crime or disorder (c) economic well-being of UK (d) public safety (e) public health

SERVICE POLICE (NAVY ARMY, AIR FORCE) AND MINISTRY OF DEFENCE POLICE

Armed Service police provide support for the navy, army and air force operating in the UK and overseas as well as policing the Services themselves. Covert techniques are used to gain intelligence to prevent and detect crime against or on Armed Service property, establishments and personnel (such as countering hostile surveillance) and any crime committed by Service officers.

The Ministry of Defence Police provide a nationwide, armed guarding role at defence sites requiring a high level of security. This includes guarding Britain's nuclear deterrent. Covert investigative powers assist them in safeguarding site perimeters, and protecting against the sabotage of assets and the threat of terrorist attack.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
The Royal Navy Police: Commander The Royal Military Police: Lieutenant Colonel The Royal Air Force Police: Wing Commander MOD Police: Superintendent	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (a) national security, (b) preventing or detecting crime or disorder (c) economic well-being of UK (g) in an emergency preventing death/ injury
The Royal Navy Police: Lieutenant Commander The Royal Military Police: Major The Royal Air Force Police: Squadron Leader MOD Police: Inspector	RIPA S21(4) (c) subscriber data	
The Royal Navy Police: Commander The Royal Military Police: Lieutenant Colonel The Royal Air Force Police: Wing Commander MOD Police: Superintendent	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) & S29(3) (a) national security (b) preventing or detecting crime or disorder (c) economic well-being of UK
The Royal Navy Police: Lieutenant Commander The Royal Military Police: Major The Royal Air Force Police: Squadron Leader MOD Police: Inspector	Urgent cases	
The Royal Navy Police: Provost Marshal The Royal Military Police: Provost Marshal The Royal Air Force Police: Provost Marshal	Where Confidential information is likely to be obtained or when a vulnerable person/juvenile is to be used as a CHIS	

SERIOUS ORGANISED CRIME AGENCY

Intelligence-led law enforcement agency which operates against the illegal drugs trade, hi-tech crime, people smuggling, counterfeiting currency and serious robberies involving firearms. The Child Exploitation and Online Protection Centre (CEOP) is an integral part of SOCA. It protects children by identifying internet sexual offenders undertaking grooming activities, tracking down convicted sex offenders who have failed to register their whereabouts, and investigating circumstances where a sexual offender is engaging with or seeking the company of children.

Proposed changes reflect developing role of SOCA.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Senior Manager (Grade 2)	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder **(g) in an emergency preventing death/injury** Article 2 (b) identifying person
Principal Officer (Grade 3)	RIPA S21(4) (c) subscriber data	
Senior Manager (Grade 2)	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder
Principal Officer (Grade 3)	Urgent cases	
Deputy Director	Where Confidential information is likely to be obtained or when a vulnerable person/juvenile is to be used as a CHIS	

HM REVENUE AND CUSTOMS

Responsible for policing/assuring a wide range of UK revenues, taxes and duties as well as protecting the public at the frontier by combating the smuggling of prohibited, restricted and duty payable items. This includes avoidance of millions of pounds of duties and taxes on goods and attacks on the self assessment and tax credit systems, where organised crime gangs with false identities use multiple claims to obtain large repayments. Also carries out investigations in the interests of national security (for instance enforcing trade sanctions and embargoes, countering the trafficking of weapons of mass destruction and in support of Project Cyclamen Operations – a cross-Departmental initiative to screen for the illicit importation of radioactive materials).

Proposed changes reflect organisational changes and priorities.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Senior Officer	RIPA S21(4) **(a) traffic data*** (b) service use (c) subscriber data * Revenue staff currently limited to traffic data for postal services only. Consolidating Order would lift this limitation	RIPA S22(2) (b) preventing or detecting crime or disorder (f) collection of taxes
Higher Officer	RIPA S21(4) (c) subscriber data	
Senior Officer	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) & S29(3) (a) national security (b) preventing or detecting crime or disorder **(c) economic well-being of UK – to be removed** (d) public safety (e) public health (f) collection of taxes
Higher Officer	Urgent cases	
Director Investigation or Regional Heads of Investigation	Where Confidential information is likely to be obtained	
Grade 7 (Intelligence)	When a vulnerable person/juvenile is to be used as a CHIS	

INTELLIGENCE AGENCIES

- Security Service
- Secret Intelligence Service
- Government Communications Headquarters

The Security Service protects UK from threats to national security (including terrorism and espionage) and helps counter proliferation of weapons of mass destruction. Its covert intelligence investigations enable it to identify, assess and counter these threats.

SIS collects UK's foreign intelligence and has a global covert capability to promote and defend the national security and UK economic well-being. It supports the Security Service's responsibilities and represents its interests with cooperating foreign intelligence agencies.

GCHQ provides signals intelligence and information assurance advice to help keep Government communication and information systems safe from hackers and other threats.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
The Security Service: General Duties 3 or any other officer at Level 3 SIS: Grade 6 or equivalent GCHQ: GC8	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (a) national security (b) preventing or detecting crime or disorder (e) economic well-being of UK
The Security Service: General Duties 4	RIPA S21(4) (c) subscriber data	
The Security Service: General Duties 3 or any other officer at Level 3 SIS: Grade 6 or equivalent GCHQ: GC8	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) & S29(3) (a) national security (b) preventing or detecting crime or disorder (c) economic well-being of UK
The Security Service: Deputy Director General SIS: A Director of the Secret Intelligence Service GCHQ: A Director of GCHQ	Where Confidential information is likely to be obtained	
The Security Service: Deputy Director General SIS: A member of the Secret Intelligence Service not below the equivalent rank to that of a Grade 5 in the Home Civil Service GCHQ: A Director of GCHQ	When a vulnerable person/juvenile is to be used as a CHIS	

ARMED SERVICES (Navy, Army, Air Force) and MINISTRY OF DEFENCE

Role is to defend the security of the UK and its Overseas Territories (including defending against terrorism). Access to RIPA enables the Services to provide life-saving intelligence in support of military operations, including information on an enemy's intentions, capabilities and modus operandi, immediate threat warning to the lives of armed forces personnel and information aiding commanders' decision-making. The Ministry of Defence acts to prevent or detect crime or disorder affecting the Armed Services.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
The Royal Navy: Commander The Army: Lieutenant Colonel The Royal Air Force: Wing Commander **MOD: Band C1** **Proposal to remove MOD**	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S22(2) (a) national security (b) preventing or detecting crime or disorder (c) economic well-being of UK (d) public safety (e) public health **MOD only** **(b) preventing or detecting crime or disorder - to be removed**
The Royal Navy: Lieutenant Commander The Army: Major The Royal Air Force: Squadron Leader **MOD: Band C2** **Proposal to remove MOD**	Urgent cases	
The Royal Navy: Rear Admiral The Army: Major General The Royal Air Force: Air-Vice Marshal **MOD: Director General or equivalent** **Proposal to remove MOD**	Where Confidential information is likely to be obtained or when a vulnerable person/juvenile is to be used as a CHIS	

OFFICE OF FAIR TRADING

The UK's consumer and competition authority uses RIPA to investigate:

- breaches of competition law and fraudulent and aggressive practices under the Competition Act 1998 and the Enterprise Act 2002, including conducting both civil and criminal investigations into cartels (regarded as amongst the most serious forms of anti-competitive behaviour, causing serious detriment to consumers and legitimate businesses cartels); and
- consumer crime (rogue traders and scams to con recipients with false or misleading claims). UK consumers lose up to £3.5b a year to rogue traders and consumer scams, including bogus lotteries and deceptive premium-rate prize promotions.

Proposed extension of the UK economic well-being purpose (which is at present limited to their use of directed surveillance and CHIS) to communications data reflects that civil offences under the Competition Act harm consumers but also prejudice other related businesses, undermining confidence in the operation of markets and impacting on the UK's economic well-being.

A change in authorising officers requested by OFT reflects the fact that the Cartels Group now additionally has responsibility for criminal enforcement in the consumer field, and that reorganisation has resulted in different job titles. The seniority and independence of the authorising officers will not change.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Any member of the Senior Civil Service with responsibility for cartels or criminal enforcement	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder **(c) economic wellbeing of UK**
Any member of the Senior Civil Service with responsibility for cartels or criminal enforcement Grade 7 in the Cartels & Criminal Enforcement Group	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder (c) economic well-being of UK

7.3 Other Public Authorities

NB. Significant proposed changes identified below in **bold.**

AMBULANCE SERVICES		
UK-wide accident and emergency service for the response to 999 calls and transport to take vulnerable patients to and from their hospital appointments. Ambulance Services across the UK use RIPA to locate callers in an emergency where the caller is unable to give their position or to contact relatives or next of kin to give relevant details of patients. RIPA is also used to investigate assaults on staff, inappropriate and hoax 999 calls.		
WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
ENGLAND Duty Manager of Ambulance Trust Control Rooms in an NHS Trust established under s5 of the NHS & Community Care Act 1990 whose functions, as specified in its Establishment Order, include the provision of emergency ambulance services	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (g) in an emergency preventing death/ injury
Director of Operations or Control and Communications Manager in an NHS Trust established under s5 of the NHS & Community Care Act 1990 whose functions, as specified in its Establishment Order, include the provision of emergency ambulance services	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
WALES Regional Control Manager in the Welsh Ambulance Services NHS Trust	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (g) in an emergency preventing death/ injury
Director of Operations in the Welsh Ambulance Services NHS Trust	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
SCOTLAND Emergency Medical Dispatch Centre Officer in Charge in the Scottish Ambulance Service Board	S21(4) (a) traffic data (b) service use (c) subscriber data	S22(2) (g) in an emergency preventing death/ injury
Director of Operations in the Scottish Ambulance Service Board	S21(4) (b) service use (c) subscriber data	S22(2) (b) preventing or detecting crime or disorder
NORTHERN IRELAND Control Supervisor in Ambulance Control Room in the Northern Ireland Ambulance Service Health & Social Services Trust	S21(4) (a) traffic data (b) service use (c) subscriber data	S22(2) (g) in an emergency preventing death/ injury
Director of Operations in the Northern Ireland Ambulance Service Health & Social Services Trust	S21(4) (b) service use (c) subscriber data	S22(2) (b) preventing or detecting crime or disorder

CHARITY COMMISSION

The statutory regulator of charities in England and Wales. Investigates charity misconduct or mismanagement such as fraud, money laundering, links to terrorist organisations, sham charities set up for improper or illegal purposes or for private advantage or the abuse of vulnerable beneficiaries. This allows the public to be confident that the money given to charities actually does go to the good causes represented.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Senior Investigations Manager	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
Senior Investigations Manager	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder
Investigations Manager	Urgent cases	

CHILD MAINTENANCE AND ENFORCEMENT COMMISSION

Set up by the Child Maintenance and Other Payments Act 2008 specifically to reinvigorate the child maintenance system carried out by the previous Child Support Agency in the Department for Work and Pensions. Role includes calculating, collecting and enforcing child maintenance liabilities. It will use directed surveillance to gather evidence against non-resident parents who misrepresent their position or refuse to engage over the question of working out equitable arrangements for the support of their children. Directed surveillance will enable investigation of these cases to be advanced by determining where the absent parent lives and works and by assessing lifestyle and wealth for use in considering maintenance payment orders.

In line with the Department for Work and pensions, CHIS authorisations are no longer required.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Senior Executive Officer or equivalent grade in the Child Maintenance & Enforcement Commission	RIPA S26(1) (a) directed surveillance **(c) conduct & use of CHIS – to be removed** **(CHIS powers not to be inherited from previous public authority responsible for this area (Child Support Agency in Dept of Work and Pensions))**	RIPA S28(3) (b) preventing or detecting crime or disorder
Higher Executive Officer or equivalent grade in the Child Maintenance & Enforcement Commission	Urgent cases	

CIVIL NUCLEAR CONSTABULARY

Protects designated civil nuclear sites by preventing or responding effectively to security breaches in segregated nuclear areas, providing secure, armed escorts for the storage and movement of civil nuclear materials in the UK and abroad, and ensuring an effective armed response in the event of terrorist targeting.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Superintendent	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (a) national security (b) preventing or detecting crime or disorder
Inspector	RIPA S21(4) (c) subscriber data	
Superintendent Inspector	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases	RIPA S28(3) & S29(3) (a) national security (b) preventing or detecting crime or disorder

CARE QUALITY COMMISSION (FORMERLY THE COMMISSION FOR HEALTHCARE AUDIT AND INSPECTION

Inspects the NHS, private and voluntary healthcare sectors in order to ensure that statutory standards of healthcare are maintained. This includes investigating unregistered or below-standard premises and inspecting for poor or dangerous practices that put the public at risk. For instance preventing or addressing hospital acquired infections such as MRSA and colostridium difficile outbreaks. Where necessary, prosecutes breaches. Under the Heath and Social Care Act 2008, a successor authority - the Care Quality Commission - will replace the Healthcare Commission with effect from April 2009 and be expected to maintain and reinvigorate strong enforcement function in these areas.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Head of Operations in a region Area Manager	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder (e) public health

CRIMINAL CASES REVIEW COMMISSION / SCOTTISH CRIMINAL CASES REVIEW COMMISSION

Investigates potential miscarriages of justice and affirms the safety of convictions, thus reinforcing everyone's right to a fair trial under ECHR and promoting confidence in the effectiveness of the criminal justice system. Their use of communications data enables them to determine salient facts to support or undermine assertions made by people claiming wrongful conviction. This includes verifying an applicant's location at the time of the crime or proving/disproving that a call was made at the material time.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
An Investigations Adviser in the Criminal Cases Review Commission / A Legal Officer in the Scottish Criminal Cases Review Commission	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	Article 2 (a) miscarriages of justice

DEPARTMENT OF AGRICULTURE AND RURAL DEVELOPMENT IN NORTHERN IRELAND

DARD has statutory enforcement responsibilities for a wide range of animal health and welfare issues in Northern Ireland, including traceability and disease control offences committed in abuse of the border with the Republic of Ireland. It uses RIPA in such areas as illegal cattle movement, the illegal importation of meat products and vetinary medicines and where necessary tracing subsidy and compensation fraud back to Department staff.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Head of Financial Policy & Investigations Services	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
NB. Directed surveillance and CHIS authorised under NI Statutory Instrument No.292 of 2002 – not included in Consolidating Orders		

DEPARTMENT FOR BUSINESS, ENTERPRISE AND REGULATORY REFORM

The competition regulator is able to use RIPA to prevent or detect crime or disorder relating to a range of anti-competive business offences. This includes investigating and prosecuting offences under the Companies Act, Insolvency Act, Fraud Act and Theft Acts such as insolvency fraud, unscrupulous trading practices and breaches in employment legislation. The effect of effective regulation is to boost UK productivity, protect the consumer, expand choice and provide better value.

Re-titling and standardisation of authorising officers required following change from Department of Trade and Industry in June 2007.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Deputy Chief Investigation Officer in the Investigation Officers Branch	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
Deputy Chief Investigation Officer in the Investigation Officers Branch The Director of Legal Services A	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Where Confidential information is likely to be obtained or when a vulnerable person/juvenile is to be used as a CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder

DEPARTMENT OF ENTERPRISE, TRADE AND INVESTMENT FOR NORTHERN IRELAND

Undertakes same functions performed by the Health and Safety Executive and local council trading standards in the rest of the UK. This includes safeguarding the interests of consumers and ensuring health, safety and welfare at work.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Deputy Chief Inspector in Trading Standards Service	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
NB. Directed surveillance and CHIS authorised under NI Statutory Instrument No.292 of 2002 - not included in Consolidating Orders		

DEPARTMENT FOR ENVIRONMENT, FOOD & RURAL AFFAIRS

DEFRA Investigation Services (DIS) enforces legislation relating to animal welfare (eg foot and mouth disease) and investigates crime and compensation and subsidy fraud covering a wide range of subjects (such as cattle identification), tree felling, veterinary medicines, use of pesticides and plant health. It uses covert techniques mainly to trace the sellers of illegal veterinary medicines and investigate offences contrary to the Dairy Produce Quota Regulations (the supply of milk outside the quota system).

The Marine and Fisheries Agency (MFA) enforces legislation governing fishing at sea, including catch-quotas, fish and mesh sizes, foreign fishing rights and the fish's journey to first sale. The benefit of offending is worth millions of pounds to individuals and disrupts the fish economy for the majority.

The Centre for Environment, Fisheries and Aquaculture Science (Cefas) enforces regulations to prevent the spread of serious disease in England and Wales freshwater fish and shellfish stocks. This applies both to stocks kept for farming and sport. Covert techniques tackle the illegal importation of fish by determining addresses of offenders and gathering evidence of illegal importation. Circumventing these controls would have potentially serious effect in terms of the spread of any fatal disease introduced to the country.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
DIS: Senior Investigation Officer MFA: Deputy Chief Inspector Cefas: Senior Investigation Officer	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
DIS: Senior Investigation Officer MFA: District Inspector (for directed surveillance) Deputy Chief Inspector (for CHIS) Cefas: Senior Investigation Officer	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder
DIS: Senior Investigation Officer MFA: Immediate Senior Officer of Head of Defra Prosecution Division	Where Confidential information is likely to be obtained	
Cefas: Immediate Senior Officer of Head of Defra Prosecution Division DIS: Head of Unit Cefas: Head of Unit of Defra Investigation Services	When a vulnerable person/juvenile is to be used as a CHIS	

DEPARTMENT OF HEALTH - MEDICINES AND HEALTHCARE PRODUCTS REGULATORY AGENCY

The MHRA is the statutory enforcement agency responsible for ensuring that medicines and medical devices are tested, work and are acceptably safe. It investigates and prosecutes:

- Breaches in the control of licensed medicines, including unlicensed or counterfeit medicines supplied on the internet, stored in warehouses or sold in retailers.
- Suppliers of counterfeit medical devices. Cases in the UK that are known to have reached consumers include condoms and dental material for use in fillings. Incidents of counterfeits intercepted before reaching consumers include glucose test strips for use in conjunction with insulin, and corrective contact lenses.

If not prevented or taken out of circulation, unlicensed, unlawful or counterfeit medicines and medical devices can lead directly to reduced quality or even loss of life.

Slight change of authorising officer to a higher grade.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Grade 7 in the Medicines & Healthcare Products Regulatory Agency	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder (d) public safety (e) public health
Grade 6 in the Medicines & Healthcare Products Regulatory Agency Grade 7 in the Medicines & Healthcare Products Regulatory Agency Chief Executive Head of Division for Inspection and Enforcement	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases Where Confidential information is likely to be obtained When a vulnerable person/juvenile is to be used as a CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder (d) public safety (e) public health

DEPARTMENT FOR TRANSPORT – ACCIDENT & INVESTIGATION BRANCHES

Different branches responsible for investigating accidents in the air, on water and rail. Investigations determine cause of accident with a view to preserving life, improving safety and preventing future occurrences. An integral part of the investigations is ascertaining whether the use of telecommunications by drivers, pilots or others played any part in the incident (which may include loss of life).

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Inspector in the Air Accident Investigation Branch, the Marine Accident Investigation Branch or the Rail Accident Investigation Branch	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (d) public safety

DEPARTMENT FOR TRANSPORT – DRIVING STANDARDS AGENCY

Responsible for setting and maintaining the standard of all driving tests in the UK, ensuring that the public is protected from untested and unqualified drivers and therefore helping to reduce road fatalities. Investigates, seeks to prevent and prosecutes people using bogus identities to take (multiple) driving tests on behalf of other people. Also tackles untested and unqualified people posing as driving instructors. Proposed change will facilitate prosecution in these cases.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Chief Executive of the Driving Standards Agency	RIPA S26(1) (a) directed surveillance **(c) conduct & use of CHIS – to be removed**	RIPA S28(3) **(b) preventing or detecting crime or disorder** (d) public safety

DEPARTMENT FOR TRANSPORT – MARITIME & COASTGUARD AGENCY

The Coastguard uses RIPA to locate people/vessels in carrying out emergency search and rescue function including missing vessels, people in distress at sea, or people at risk of injury or death on UK cliffs or shoreline.

The Enforcement Branch uses RIPA to investigate and prosecute breaches of the Maritime Shipping Act (relating to the safe construction and operation of both cargo and passenger craft) and anti-pollution legislation (including tracing responsibility for and taking action against those responsible for oil or chemical spills).

Proposed changes assist in locating missing/vulnerable people in circumstances that do not constitute the emergency prevention of death or injury, and to ensure 24 hour cover.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
COASTGUARD Area Operations Manager in the Maritime & Coastguard Agency	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (g) in an emergency preventing death/ injury
Rescue Co-ordination Centre Manager in the Maritime & Coastguard Agency	RIPA S21(4) (c) subscriber data	
ENFORCEMENT BRANCH Principal Enforcement Officer in the Maritime and Coastguard Agency	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder (d) public safety
Enforcement Officer in the Maritime and Coastguard Agency	RIPA S21(4) (c) subscriber data	
ENFORCEMENT BRANCH Principal Enforcement Officer in the Maritime & Coastguard Agency Enforcement Officer in the Maritime & Coastguard Agency	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases	RIPA S28(3) (b) preventing or detecting crime or disorder (d) public safety

DEPARTMENT FOR TRANSPORT – VEHICLE & OPERATOR SERVICES AGENCY

Provides a range of licensing, testing and enforcement services to improve the roadworthiness standards of both private and commercial vehicles. Covert activity protects the public from serious injury or death on the roads by:

- Investigating garages fraudulently issuing private vehicle MOT certificates for roadworthiness. This includes assembling evidence where necessary to remove garages' authorisation to conduct MOT examinations as well as pressing for the prosecution of individuals.
- Investigating the illegal operation of goods vehicles, such as operating without licence, overloading vehicles and abusing drivers' hours legislation.

Slight change: Higher authorisation levels recommended by internal review following Office of Surveillance Commissioners' advice.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Head of Intelligence, Head of Investigations or Regional Operations Manager in VOSA	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) (b) preventing or detecting crime/ disorder (d) public safety
Area Manager or Regional Intelligence Co-ordinator in VOSA	Urgent cases (directed surveillance)	
Regional Intelligence Co-ordinator in VOSA	Urgent cases (CHIS)	

DEPARTMENT FOR WORK AND PENSIONS

RIPA used to assist Jobcentre Plus staff investigate employment benefit fraud (as opposed to local authorities who investigate housing benefit and council tax fraud). This includes income support, jobseeker's allowance, pension credit, incapacity benefit and employment support. Directed surveillance tracks organised gangs in major counterfeiting and multiple identity attacks on the benefit system and helps investigations relating to smaller scale fraud such as undeclared working and living together. It also enables the DWP Risk Assurance Division to investigate fraud where DWP staff are complicit.

Proposed changes reflect the DWP's policy to not deploy CHIS.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Senior Executive Officer or equivalent grade in Jobcentre Plus Senior Executive Officer or equivalent grade in DWP Risk Assurance Division	RIPA S26(1) (a) directed surveillance **(c) conduct & use of CHIS – to be removed**	RIPA S28(3) (b) preventing or detecting crime or disorder
Higher Executive Officer or equivalent grade in Jobcentre Plus	Urgent cases	
Chief Executive of Jobcentre Plus	Where Confidential information is likely to be obtained	

ENVIRONMENT AGENCY / SCOTTISH ENVIRONMENT PROTECTION AGENCY

The leading public bodies for environmental regulation and advice in England, Wales and Scotland. Responsible for combating pollution and protecting and improving the environment. Main focus is public health and safety, including large-scale illegal waste dumping, the running of unregulated landfill sites and trespassers jeopardising their and others safety by tampering with gas generated by waste and stored on site. Also tackle organised criminals perpetrating large-scale, geographically dispersed environmental crimes, including international illegal exports of waste.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Area Management Team Member in the Environment Agency / Any Director in the Scottish Environment Protection Agency	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder (d) public safety (e) public health
Area Management Team Member Area Team Leader	RIPA S26(1) (a) directed surveillance Urgent cases	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder (d) public safety (e) public health
Area Manager National Enforcement Service Manager Chief Executive of the Environment Agency Executive Manager in the Environment Agency *Scottish Environmental Protection Agency authorisation of directed surveillance and CHIS is under RIP(S)A – not included in Consolidating Orders*	RIPA S26(1) (c) conduct & use of CHIS Urgent cases Where Confidential information is likely to be obtained When a vulnerable person/juvenile is to be used as a CHIS	

FINANCIAL SERVICES AUTHORITY

The UK's financial regulator with statutory responsibilities for investigating and prosecuting particular criminal offences to maintain market confidence. RIPA used mainly in the investigation and prosecution of insider dealing under the Criminal Justice Act 1993. Other investigations in which covert techniques have been used include unauthorised collective investment schemes under the Financial Services and Markets Act 2000. The FSA is increasingly involved in detecting criminal activity on the internet. Unless these kinds of professional financial collaboration are addressed effectively they would operate against the consumer's interests and could damage the integrity of UK financial markets.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Head of Department in Enforcement Division	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
Head of Department in Enforcement Division Manager in Enforcement Division Chairman of the Financial Services Authority	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases Where Confidential information is likely to be obtained or when a vulnerable person/juvenile is to be used as a CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder

FIRE AND RESCUE SERVICES

Fire and rescue services across the UK attend fire incidents at domestic and commercial premises (including oil and gas terminals, power stations, airports, docks etc) and serious road accidents. They are also responsible for enforcing regulations concerning fire safety. This work enables them to save lives and protect property and the environment. Covert techniques are used in connection with taking enforcement action in support of explosive and petroleum regulations or deliberate fire setting to help piece together the sequence of events, progressing accident investigations (for instance where fire fighters are injured at the scene of a fire) and detecting hoax calls.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Fire Control Officer	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (g) in an emergency preventing death/injury
Group Manager or Principal Fire Control Officer	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder (d) public safety
Group Manager	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder (d) public safety

FOOD STANDARDS AGENCY

Created under the Food Standards Act 1999 to protect the public by enforcing statutory food safety standards. Inspects meat at slaughterhouses and processing plants to ensure that the standards required by the law for hygienic production and animal welfare at slaughter are maintained. Its enforcement team consider the use of RIPA to prevent unfit meat from entering the market for human consumption. If it did not have covert techniques to use when it needed to, there could be serious public health consequences and the consequences for some consumers could be fatal.

The proposed changes reflect the Agency's belief that it can operate effectively against illicit meat diversion from slaughterhouses using crime and public health RIPA purposes only.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Deputy Director of Legal Services or any Director	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder **(d) public safety - to be removed** (e) public health
Head of Division or equivalent grade	RIPA S26(1) (a) directed surveillance	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder **(d) public safety - to be removed** (e) public health
Deputy Director of Legal Services or any Director Head of Group, Deputy Chief Executive and Chief Executive of the Food Standards Agency *In Northern Ireland directed surveillance and CHIS are authorised under NI Statutory Rule No.292 of 2002 - not included in Consolidating Orders*	RIPA S26(1) (c) conduct & use of CHIS Where Confidential information is likely to be obtained or when a vulnerable person/juvenile is to be used as a CHIS	

GAMBLING COMMISSION

Set up under the Gambling Act 2005 to regulate the gambling industry in Great Britain, including the licensing and operation of casinos, bingo, gaming machines and lotteries (on site, telephone and internet gambling). It has used covert techniques mostly to investigate and close down unregulated poker clubs which do not afford adequate protection against violence or intimidation, the involvement of children and vulnerable people, extortion and cheating, or allowing individuals to choose when to stop participating.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Director of Intelligence or Director of Monitoring and Enforcement	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
Director of Intelligence or Director of Monitoring and Enforcement	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder

GANGMASTERS LICENSING AUTHORITY

Established under the Gangmasters (Licensing) Act 2004 following public concern at the lack of action to prevent the deaths of migrant cockle pickers in Morecambe Bay. The GLA issues licenses only to approved gangmasters and investigates/prosecutes those without a license. Covert techniques allow them to link unapproved gangmasters to the migrants they are exploiting. It is important that the problem is addressed by taking effective action against both labour providers and labour users that exploit illegal migrant workers.

Minor change to the title of the authorising officer reflecting reorganisation in operational structure.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Head of Operations	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
Head of Operations	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder

HEALTH AND SAFETY EXECUTIVE

The enforcement authority for most work-related health and safety legislation. Investigates and prosecutes offences which involve the creation of serious risks to people's health and safety such as poisonings, explosions from faulty domestic gas installations, major chemical incidents (such as the one at Buncefield), movement of dangerous goods and construction site injuries etc. RIPA authorisations enable the HSE to trace individuals and companies whose activities are putting people at risk of serious harm.

Proposed Changes

Ability to authorise CHIS would enable HSE to continue the effective investigation of an area recently transferred to it by Defra and for which Defra used CHIS. This involves taking action against the illegal trade in unapproved and dangerous pesticides where test purchases are made by undercover officers conducting investigations to trace the source of supply and prosecute those responsible. These operations involve developing relationships with the targets (either by telephone or face to face) over a period of time and therefore require covert human intelligence source authorisations.

HSE accept that the RIPA purpose 'in an emergency to prevent death or injury' is not applicable to them as it is not a front line emergency service.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Band 2 Inspector	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder (d) public safety (e) public health **(g) in an emergency preventing death/injury – to be removed**
Band 2 Inspector Director of Field Operations, Director of Hazardous Installations Directorate, or HM Chief Inspector of Nuclear Installations	RIPA S26(1) (a) directed surveillance **(c) conduct & use of CHIS** Where Confidential information is likely to be obtained or when a vulnerable person/juvenile is to be used as a CHIS	RIPA S28(3) (b) preventing or detecting crime or disorder (d) public safety (e) public health

HM CHIEF INSPECTOR OF EDUCATION, CHILDREN'S SERVICES AND SKILLS

Regulatory authority for children in care and the prosecution authority for childcare providers operating without registration. Investigates criminal offences under the Children Act 1989, Care Standards Act 2000 and the Childcare Act 2006 to ensure all children in regulated care are safe. For example, investigates unregistered or suspended childminders operating childcare services or providing childcare in breach of the law (such as exceeding permissible numbers of children) where there is no other way of ensuring that statutory regulations are being observed.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Principal Officer, Compliance, Investigations and Enforcement Team	RIPA S26(1) (a) directed surveillance	RIPA S28(3) (b) preventing or detecting crime or disorder

HOME OFFICE

i) UK Border Agency outward looking immigration crime teams investigate offences against the Immigration Acts, such as overstaying leave to enter or remain, contacting bogus marriages or organised groups masterminding people trafficking for prostitution or forced labour.

ii) UKBA inward looking anti-corruption teams investigate UKBA staff suspected of conducting or colluding in immigration crime.

iii) UKBA asylum fraud teams investigate the abuse of the system of support and benefits to asylum seekers where the public interest is to pursue and stop benefit cheats who steal from the genuinely deserving.

iv) Removal centres are responsible for escorting & holding people detained under immigration law and assisting in the removal of those not entitled to stay.

Proposed changes reflect organisational changes.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
i) immigration crime Immigration Inspector in the UK Border Agency	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
ii) anti-corruption Immigration Inspector or Senior Executive Officer with responsibility for anti-corruption in the UK Border Agency	**RIPA S21(4)** **(a) traffic data** **(b) service use** **(c) subscriber data**	**RIPA S22(2)** **(b) preventing or detecting crime or disorder**
iii) asylum fraud Immigration Inspector with responsibility for asylum fraud investigations in the UK Border Agency	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
iv) Immigration removal centres Security Liaison Director in the UK Border Agency or Security Liaison Director in a contracted out removal centre	**RIPA S21(4)** **(a) traffic data** **(b) service use** **(c) subscriber data**	**RIPA S22(2)** **(b) preventing or detecting crime or disorder** **(d) public safety** **Article 2** **(b) identifying person**

i) <u>immigration crime</u> Immigration Inspector in the UK Border Agency Chief Immigration Officer in the UK Border Agency Strategic Director of the UK Border Agency or (in his/her absence) Director in the UK Border Agency Intelligence Directorate Strategic Director of the UK Border Agency	RIPA S26 (1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases Where Confidential information is likely to be obtained When a vulnerable person/juvenile is to be used as a CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder (c) economic well-being of the UK
<u>ii) anti-corruption</u> The Head of the Unit responsible for anti-corruption in the UK Border Agency Senior Executive Officer in the Unit responsible for anti-corruption in the UK Border Agency Strategic Director of the UK Border Agency or (in his/her absence) Director in the UK Border Agency Intelligence Directorate	RIPA S26 (1) (a) directed surveillance Urgent cases Where Confidential information is likely to be obtained	RIPA S28(3) (b) preventing or detecting crime or disorder
iii) <u>asylum fraud</u> N/A	N/A	N/A
iv) <u>Immigration Removal Centres</u> Security Liaison Director in the UK Border Agency or Security Liaison Director in a contracted out removal centre	**RIPA S26(1)** **(a) directed surveillance** **(c) conduct & use of CHIS**	**RIPA S28(3) & S29(3)** **(b) preventing or detecting crime or disorder** **(d) public safety**

INDEPENDENT POLICE COMPLAINTS COMMISSION

Took over in 2004 from Police Complaints Authority to oversee the handling of public complaints of misconduct against the police and other law enforcement bodies. Its independent role from law enforcement agencies means it needs its own investigative powers. Where someone dies as a result of contact with a law enforcement agency the agency itself is required to notify the IPCC who conducts the investigation on behalf of the coroner. It is these cases where the use of RIPA can help identify the victim and his location at the time of the incident and enables family or friends to be contacted to establish his state of mind at the time.

Proposed changes required to i) discharge the IPCC's obligations in coroners' cases to investigate misconduct where the nature of misconduct does not constitute a crime and ii) reflect streamlining of organisation.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Commissioner or Regional Director	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder **Article 2** **(b) identifying person**
Regional Director Senior Investigating Officer	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder

INFORMATION COMMISSIONER

Oversees compliance with the provisions of the Data Protection Act 1998, the Freedom of Information Act 2000 and the Privacy & Electronic Communications Regulations 2003. Personal information has a financial value and can be traded for criminal purposes to the detriment of the individual whose data is stolen and misused, and for society at large. The Commissioner's Office uses covert techniques where necessary to assist in identifying offenders attempting unlawfully to obtain, disclose, sell or offer to sell personal data in contravention of the above legislation.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Head of Investigations	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
Head of Investigations Senior Investigating Officer	RIPA S26(1) (a) directed surveillance Urgent cases	RIPA S28(3) (b) preventing or detecting crime or disorder

LOCAL AUTHORITIES

353 local authorities in England, 22 in Wales, 32 in Scotland and 26 in Northern Ireland are able to use service use and subscriber data in order to prevent or detect crime or disorder in connection with their statutory functions. Many of these functions are their sole responsibility.

Examples of investigations where covert techniques enable local authorities to trace investigations back to a source individual at a specific address and offer evidence against them in legal proceedings include:

- trading standards (eg action against loan sharks and rogue traders, car fraud, consumer scams, deceptive advertising, counterfeit goods, unsafe toys and electrical goods);
- enforcement of anti-social behaviour orders and legislation relating to unlawful child labour;
- housing/planning (eg intervening to stop and take remedial action against unregulated and unsafe building, breaches of preservation orders, cases of landlord harassment);
- benefits fraud (eg housing benefits, investigating 'living together' and 'working whilst in receipt of benefit' allegations, council tax evasion); and
- environment protection (eg action to stop large-scale waste dumping, the sale of unfit food and illegal 'raves').

The advantages of being able to use communications data to help criminal investigation especially in trade and consumer scams is becoming more important with the growth of the internet and distance selling. Many transactions are now done without buyer and seller coming into contact and the only way of linking offenders to these transactions is by communications data.

A series of media articles last year reported some local authorities' use of covert techniques against activities such as dog fouling and littering. The Government and the Local Council Association have separately made it clear that using RIPA authorisations in these instances would not be a proportionate response. The Home Office is working closely with the Department for Communities and Local Government and the relevant Commissioners to address instances of inappropriate use of covert techniques. The statutory RIPA Codes of Conduct which provide guidance to practitioners are being revised accordingly.

Some media articles have confused what RIPA allows local authorities to do with the more intrusive forms of covert activity conducted by intelligence and law enforcement agencies. *Under RIPA local authorities cannot intercept communications (such as telephone 'tapping' or reading someone's e-mails, texts or post) or enter anyone's house covertly. RIPA limits these covert activities to those public authorities with a national security remit or which are operating against a level of 'serious' crime substantially above that tackled by local authorities.*

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
<u>ENGLAND, WALES, SCOTLAND & N IRELAND</u> Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
<u>ENGLAND & WALES</u> Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent The Head of Paid Service or (in his/her absence) a Chief Officer <u>SCOTLAND</u> *Directed surveillance and CHIS authorised under RIP(S)A – not included in these Consolidating Orders* <u>N IRELAND</u> *Directed surveillance and CHIS authorised under NI Statutory Rule No.292 of 2002 – not included in these Consolidating Orders*	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Where Confidential information is likely to be obtained or when a vulnerable person/juvenile is to be used as a CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder

MINISTRY OF JUSTICE

Responsible for holding prisoners securely, reducing the risk of prisoners re-offending and providing safe and well-ordered detention establishments. Proposed changes to assist investigations into deaths in custody and to reflect organisational changes such as the increasing role of contracted out prisons.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Directly managed prisons Manager in the National Intelligence Unit of the National Offender Management Service	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder (d) public safety **Article 2** **(b) identifying person**
Contracted out prisons Manager in the National Intelligence Unit of the National Offender Management Service	**RIPA S21(4)** **(a) traffic data** **(b) service use** **(c) subscriber data**	**RIPA S22(2)** **(b) preventing or detecting crime or disorder** **(d) public safety** **Article 2** **(b) identifying person**
Directly managed prisons Operational Manager responsible for security and operations in the directly managed prison	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder (d) public safety
Duty Governor in the directly managed prison	Urgent cases	
Chief Operating Officer in the National Offender Management Service	Where Confidential information is likely to be obtained	
A senior civil servant in the National Offender Management Service not below the equivalent rank of a Grade 5 in the Home Civil Service	When a vulnerable person/juvenile is to be used as a CHIS	
Contracted out prisons A Controller in the contracted out prison	**RIPA S26(1)** **(a) directed surveillance** **(c) conduct & use of CHIS**	**RIPA S28(3) & S29(3)** **(b) preventing or detecting crime or disorder** **(d) public safety**
A Deputy Controller in the contracted out prison	Urgent cases	
Chief Operating Officer in the National Offender Management Service	Where Confidential information is likely to be obtained	
A senior civil servant in the National Offender Management Service not below the equivalent rank of a Grade 5 in the Home Civil Service	When a vulnerable person/juvenile is to be used as a CHIS	

NHS SERVICES		
Three regional bodies (covering England/Wales, Scotland and Northern Ireland) work to counter fraud and corruption in the NHS - either by practitioners, patients, staff or contractors - which cheats taxpayers and takes valuable resources away from patient care. The England/Wales body - the Counter Fraud and Security Management Services Division of the NHS Business Services Authority - also investigates breaches in security which put patients and NHS assets at risk.		
WHO? (Authorisation Grade)	**WHAT? (Covert Technique)**	WHY? (Statutory Purpose)
ENGLAND AND WALES Senior Manager (not below the grade of Agenda for Change pay band 8b) in the Counter Fraud and Security Management Services Division SCOTLAND Head of NHS Scotland Counter Fraud Services NORTHERN IRELAND Head of the Counter Fraud Unit	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
ENGLAND AND WALES Senior Manager (not below the grade of Agenda for Change pay band 8b) in the Counter Fraud and Security Management Services Division Managing Director of the NHS Counter Fraud and Security Management Services Division of the NHS Business Services Authority SCOTLAND *Directed surveillance authorised under RIP(S)A – not included in these Consolidating Orders* NORTHERN IRELAND *Directed surveillance authorised under NI Statutory Rule No.292 of 2002 – not included in these Consolidating Orders*	RIPA S26(1) (a) directed surveillance Where Confidential information is likely to be obtained	RIPA S28(3) (b) preventing or detecting crime or disorder

NORTHERN IRELAND OFFICE

Northern Ireland Prison Service is responsible for holding prisoners securely, reducing the risk of prisoners re-offending and providing safe and well-ordered detention establishments. Proposed changes to assist investigations into deaths in custody and to reflect organisational changes such as the increasing role of contracted-out prisons.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Governor 4 in the Northern Ireland Prison Service	**RIPA S21(4)** **(a) traffic data** **(b) service use** **(c) subscriber data**	**RIPA S22(2)** **(b) preventing or detecting crime or disorder** **(d) public safety** **Article 2** **(b) identifying person**
Deputy Principal or Governor 3 in the Northern Ireland Prison Service Staff Officer or Governor 4 in the Northern Ireland Prison Service Director or Deputy Director, Operations, in the Northern Ireland Prison Service	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases Where Confidential material is likely to be obtained or when vulnerable person/ juvenile is to be used as a CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder (d) public safety

OFFICE OF COMMUNICATIONS

The independent regulator and competition authority for all the UK communications industries, with responsibilities across television, radio, telecommunications and wireless communications services. It uses RIPA to investigate the location and operation of illegal radio broadcasters under the Wireless Telegraphy Act 2006. This essentially means people who buy equipment from the internet and set up hidden studios to broadcast at any frequency in the radio spectrum regardless of whether that frequency is already licensed to a legitimate station. These unlicensed operators pay no taxes, provide unfair competition, interfere with legitimate broadcasters and their audiences, and disrupt vital safety of life emergency services.

Slight change to the title of the authorising officer is proposed in order to reflect a reorganisation in field operations (no change in grade).

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Spectrum Services Policy Manager	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
Field Operations Principal Field Operations Investigation Manager	RIPA S26(1) (a) directed surveillance directed surveillance urgent cases	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder
Director of Field Operations	RIPA S26(1) (c) conduct & use of CHIS	

OFFICE OF THE POLICE OMBUDSMAN FOR NORTHERN IRELAND

Investigates complaints of criminality and serious misconduct made against the Police Service of Northern Ireland, Belfast Airport Police, Harbour Police and MOD Police operating in Northern Ireland. Uses its own investigative powers so that its investigations are independent of the police services it is investigating.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Senior Investigating officer	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
Senior Investigating Officer Deputy Senior Investigating Officer	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder

PENSIONS REGULATOR

Responsible under the Pensions Act 2004 for the proper running of occupational pension schemes. The Regulator enforces employers' responsibilities to offer proper workplace pensions without penalty and to maintain the system of payments as arranged. RIPA authorisations allow tracking of illegally transferred funds from genuine company pension arrangements into bogus schemes by unscrupulous individuals operating on the internet (so-called 'pension liberators'). Sanctions include disqualifying pensions' scheme trustees, imposing fines and appointing new trustees to pension schemes in difficulty.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Regulatory Manager	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder

PORTS POLICE (MERSEYSIDE and DOVER)

Responsible for law enforcement and the security of passengers and staff in the port areas. Provide round the clock policing, investigative and prosecuting services to the owners, tenants and users of shipping premises, ferry and cruise terminals. They investigate all offences committed in the port areas but receive specialist support and assistance from other police forces when required.

Proposed changes reflect new working arrangements in which tasks are shared with other police forces listed under section 2 Police Act 1996.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Superintendent	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) **(a) national security - to be removed from both forces** (b) preventing or detecting crime or disorder (d) public safety (e) public health Article 2 (b) identifying person
Inspector	RIPA S21(4) (c) subscriber data	
Superintendent Inspector	RIPA S26(1) (a) directed surveillance **(c) conduct & use of CHIS – to be removed from Port of Dover Police only** Urgent cases	RIPA S28(3) & S29(3) **(a) national security - to be removed from both forces** (b) preventing or detecting crime or disorder (d) public safety (e) public health

POSTAL SERVICES COMMISSION

The independent regulator for postal services in the UK which acts to protect the interests of the postal industry and its users. It uses RIPA to investigate breaches of the Postal Services Act 2000. These relate to offences of unauthorised postal operations, including:

- unlawfully collecting, conveying and delivering mail without a licence; and
- interfering with mail (e.g. intentionally delaying or opening a postal packet) in the course of its transmission.

Proposed Changes reflect that the Regulator no longer needs to use directed surveillance or CHIS.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Legal Adviser	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data Limited to CD relating to a postal service	RIPA S22(2) (b) preventing or detecting crime or disorder
	RIPA S26(1) **(a) directed surveillance - to be removed** **(c) conduct & use of CHIS - to be removed**	**RIPA S28(3) & S29(3)** **(b) preventing or detecting crime or disorder – to be removed**

ROYAL MAIL

Uses RIPA to investigate and prosecute people who steal mail from the postal system and its customers. This includes passports and identity information as well as financial items and valuables, postage evasion fraud and people selling stolen goods on the internet. Communications data can help identify and locate the people using the stolen items, directed surveillance can observe and record staff suspected of theft as they work in mail processing centres or passing the items to accomplices outside the office.

Proposed changes reflect change in operational need to deploy covert human intelligence sources.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Senior Investigation Manager	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
Senior Investigation Manager Director of Security	RIPA S26(1) (a) directed surveillance **(c) conduct & use of CHIS - to be removed** Where Confidential information is likely to be obtained	RIPA S28(3) (b) preventing or detecting crime or disorder

ROYAL PHARMACEUTICAL SOCIETY OF GREAT BRITAIN

Regulatory body for pharmacists in England, Scotland and Wales. Enforces legislation applying to the people and premises involved in the sale/supply of medicines and handling of controlled drugs and hazardous chemicals. Ensures that controlled drugs, poisons and prescription medicines are managed and traded in accordance with relevant legislation and by correctly authorised individuals. Where necessary, breaches are prosecuted.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Director (Grade 7) Deputy Registrar and Director of Regulation	RIPA S26(1) (a) directed surveillance Where Confidential information is likely to be obtained	RIPA S28(3) (b) preventing or detecting crime or disorder (d) public safety (e) public health

SCOTTISH CRIME AND DRUG ENFORCEMENT AGENCY

National police agency in Scotland responsible for disrupting and dismantling serious organised crime groups, including by taking the profit out of such crime.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Superintendent or Grade PO7	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder (d) public safety (g) in an emergency preventing death/ injury
Inspector	RIPA S21(4) (c) subscriber data	
Superintendent or Grade PO7 Inspector Under RIP(S)A: Chief Constable in the area in which the proposed activity is to be undertaken Under RIP(S)A: Director	RIPA S26 (1) (a) directed surveillance (c) conduct & use of CHIS Urgent cases Where Confidential information is likely to be obtained When a vulnerable person/juvenile is to be used as a CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder (d) public safety (g) in an emergency preventing death// injury

SERIOUS FRAUD OFFICE

Set up by the Criminal Justice Act 1987 to investigate and prosecute serious or complex fraud in cases where monies at risk are at least £1m, there is a national concern or a significant international dimension or the investigation requires highly specialist skills. It operates mainly in the fields of market manipulation, fraudulent share dealing and 'dial through', concealed frauds. Sums 'at risk' in the 60 cases it investigated in 2007/08 were estimated at £4.8 billion. 65% of SFO investigations have international dimensions, and a further £30 billion of 'at risk' sums were investigated in 2007/08 responding to overseas requests for mutual legal assistance. The SFO's work reduces fraud and the cost of fraud. This enables confidence in the UK's business and financial institutions to be maintained.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Assistant Director for the Operations Division	RIPA S21(4) (a) traffic data (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
Assistant Director Director or Assistant Director	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Where Confidential information is likely to be obtained or when a vulnerable person/juvenile is to be used as a CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder

WELSH ASSEMBLY GOVERNMENT

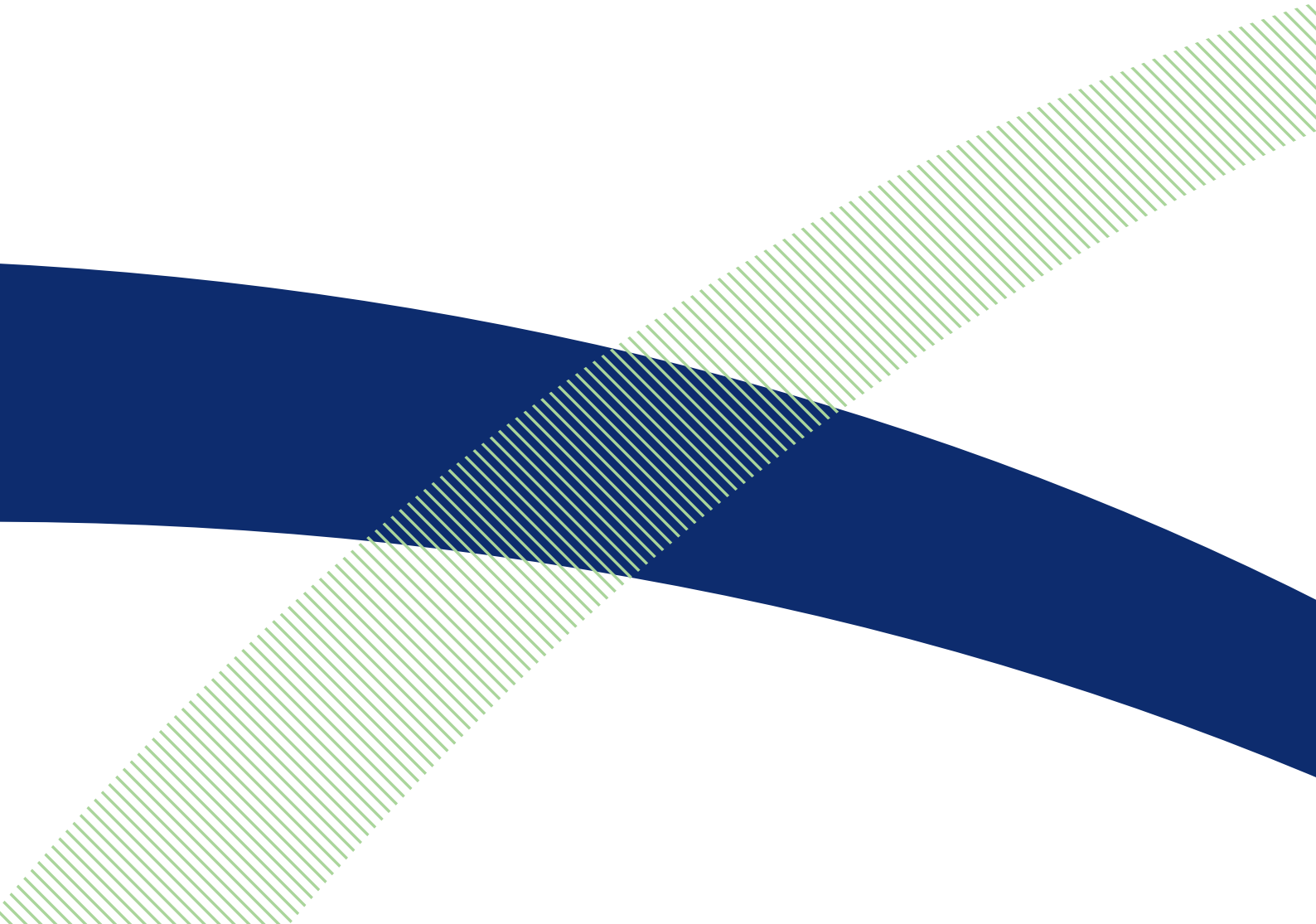
Has overall responsibility for investigations in such areas as investigating breach of regulations or registration in health and social care (including inspection of care and children's homes, day care and childminders, hospitals and clinics) and whether farmers are complying with EC and domestic legislation which regulates the subsidies they have claimed. Changes to the titles of authorising officers reflect Departmental re-organisations. Fisheries Unit now undertakes responsibilties previously undertaken in Wales by Defra.

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
Head of Department for Health & Social Services Head of Dept for Health & Social Services Finance Head of Rural Payments Division Regional Director or equivalent grade in the Care & Social Services Inspectorate for Wales Head of Fisheries Unit	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS	RIPA S28(3) (b) preventing or detecting crime or disorder (d) public safety (e) public health RURAL PAYMENTS DIVISION LIMITED TO: RIPA S28(3) (b) preventing or detecting crime or disorder (e) public health **FISHERIES UNIT LIMITED TO:** **RIPA S28(3)** **(b) preventing or detecting crime or disorder**
Member of Department for Health & Social Services at a level equivalent to Grade 7 Member of Department for Health & Social Services Finance at a level equivalent to Grade 7 Member of Rural Payments Division at a level equivalent to Grade 7 Regulation Manager or equivalent grade in the Care & Social Services Inspectorate for Wales	Urgent cases	
Head of Department for Health & Social Services Head of Dept for Health & Social Services Finance Head of Rural Payments Division Regional Director or equivalent grade in the Care & Social Services Inspectorate for Wales	Where Confidential information is likely to be obtained or when a vulnerable person/juvenile is to be used as a CHIS	

Home Office

8. Draft Code of Practice on Covert Surveillance and Property Interference

Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000



1. Introduction

Definitions

1.1. In this code:

- "1989 Act" means the Security Service Act 1989;
- "1994 Act" means the Intelligence Services Act 1994;
- "1997 Act" means the Police Act 1997;
- "2000 Act" means the Regulation of Investigatory Powers Act 2000;
- "RIP(S)A" means the Regulation of Investigatory Powers (Scotland) Act 2000.
- Terms in italics are defined in the Glossary at the end of this code.

Background

1.2. This code of practice provides guidance on the use by *public authorities* of Part II of the 2000 Act to **authorise covert surveillance that is likely to result in the obtaining of private information about a person.** The code also provides guidance on **entry on, or interference with, property or with wireless telegraphy** by *public authorities* under section 5 of the Intelligence Services Act 1994 or Part III of the Police Act 1997.

1.3. This code is issued pursuant to Section 71 of the 2000 Act, which stipulates that the *Secretary of State* shall issue one or more **codes of practice** in relation to the powers and duties in Parts I to III of the 2000 Act, section 5 of the 1994 Act and Part III of the 1997 Act. This code replaces the previous code of practice issued in 2002.

1.4. This code is publicly available and should be readily accessible by *members* of any relevant *public authority*[1] seeking to use the 2000 Act to authorise **covert surveillance that is likely to result in the obtaining of** *private information* **about a person** or section 5 of the 1994 Act or Part III of the 1997 Act to authorise **entry on, or interference with, property or with wireless telegraphy**[2].

1.5. Note that where covert surveillance activities are unlikely to result in the obtaining of *private information* about a person, or where there is a separate legal basis for such activities, this code need not apply[3].

Effect of code

1.6. The 2000 Act provides that all codes of practice relating to the 2000 Act are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers 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. *Public authorities* may also be required to justify, with regard to this code, the use or granting of *authorisations* in general or the failure to use or grant authorisations where appropriate.

1.7. Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are not provisions of the code, but are included for guidance only.

1 Being those specified in Schedule 1 to the 2000 Act (including those added to Schedule 1 by order of the *Secretary of State* under section 30 of that Act).

2 Being, at the time of writing, the Security Service, the Intelligence Service and GCHQ, the police, services police, Serious Organised Crime Agency, Scottish Crime and Drug Enforcement Agency, HM Revenue and Customs and Office of Fair Trading.

3 See Chapter 2

Surveillance activity to which this code applies

1.8. Part II of the 2000 Act provides for the authorisation of **covert surveillance** by *public authorities* where that surveillance is **likely** to result in the **obtaining of private information** about a person.

1.9. Surveillance, for the purpose of the 2000 Act, includes **monitoring, observing or listening to persons, their movements, conversations or other activities and communications**. It may be conducted with or without the assistance of a surveillance device and includes the **recording** of anything monitored, observed or listened to in the course of the surveillance[4].

1.10. Surveillance is **covert** if, and only if, it is is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place[5].

1.11. Specifically, covert surveillance may be authorised under the 2000 Act if it is either **intrusive** or **directed**:

- **intrusive surveillance** is **covert surveillance** that is carried out in relation to anything taking place on **residential premises** or in any **private vehicle** (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device);[6]
- **directed surveillance** is **covert surveillance** that is not intrusive but is carried out in relation to a specific investigation or operation in such a manner as is **likely** to result in the obtaining of *private information* about any person (other than by way of an **immediate response** to events or circumstances such that it is not reasonably practical to seek authorisation under the 2000 Act).

1.12. Chapter 2 of this code provides a fuller description of directed and intrusive surveillance, along with definitions of terms, exceptions and examples.

Basis for lawful surveillance activity

1.13. The Human Rights Act 1998 gave effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, such as the prohibition on torture, while others are qualified, meaning that it is permissible for the state to interfere with those rights if certain conditions are satisfied. Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when *public authorities seek to* obtain *private information* about a person by means of covert surveillance. Article 6 of the ECHR, the right to a fair trial, may also be engaged where a prosecution follows an investigation involving the use of covert techniques, particularly where defence counsel seek disclosure in order to challenge the lawfulness of a Part II authorisation and/or the prosecution seek to protect the use of those techniques through public interest immunity procedures.

1.14. P1.14. Part II of the 2000 Act provides a statutory framework under which covert surveillance activity can be authorised and conducted compatibly with Article 8. However, where such surveillance would not be likely to result in the obtaining of any *private information* about a person, no interference with Article 8 rights should occur and an *authorisation* under the 2000 Act is therefore not appropriate.

1.15. Similarly, an *authorisation* under the 2000 Act is not required if a *public authority* has another clear legal basis for conducting covert surveillance likely to result in the obtaining of *private information* about a person which satisfies the requirements of Article 8. For example the Police and Criminal Evidence Act 1984[7] provides a legal basis for the police covertly to record images of a suspect for the purposes of identification and obtaining certain evidence.

4 See section 48(2) of the 2000 Act
5 As defined in section 26(9)(a) of the 2000 Act
6 See Chapter 2 for full definition of residential premises and private vehicles
7 and section 76 of the Police & Criminal Evidence (Northern Ireland) Order 1989

1.16. Chapter 2 of this code provides further guidance on what constitutes *private information* and examples of activity for which *authorisations* under Part II of the 2000 Act are or are not required.

Relevant public authorities

1.17. Only certain *public authorities* may apply for *authorisations* under the 2000, 1997 or 1994 Acts:

- **Directed surveillance** *applications* may only be made by those *public authorities* listed in or added to Part I and Part II of schedule 1 of the 2000 Act.
- **Intrusive surveillance** *applications* may only be made by those *public authorities* listed in or added to section 32(6) of the 2000 Act, or by those *public authorities* listed in or designated under section 41(1) of the 2000 Act.
- *Applications* to **enter on, or interfere with, property or with wireless telegraphy** may only be made (under Part III of the 1997 Act) by those *public authorities* listed in or added to section 93(5) of the 1997 Act; or (under section 5 of the 1994 Act) by the intelligence services.

Scotland

1.18. Where **all** the conduct authorised is likely to take place in **Scotland**, *authorisations* should be granted under RIP(S)A 2000, unless the *authorisation* is being obtained by those public authorities listed in section 46(3) of the 2000 Act and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2007, SI 2007/934.

1.19. Additionally, any *authorisation* granted or renewed (by any relevant *public authority*) for the purposes of **national security or the economic well-being of the United Kingdom** must be made under the **2000 Act**, since these are reserved matters.

1.20. This code of practice is extended to Scotland in relation to *authorisations* granted under Part II of the 2000 Act which apply to Scotland. A separate code of practice applies in relation to *authorisations* granted under RIP(S)A.

International considerations

1.21. *Authorisations* under the 2000 Act can be given for surveillance both inside and outside the United Kingdom. However, *authorisations* for actions outside the United Kingdom can only render such actions lawful for the purposes of civil or criminal proceedings in or before any court or tribunal subject to the jurisdiction of the United Kingdom[8]. An authorisation under Part II of the 2000 Act does not take into account the requirements of the law of the country outside the United Kingdom in which the investigation or operation is taking place and can only render such activities lawful as a matter of English law. The laws of the relevant country must therefore be considered

1.22. *Public authorities* are therefore advised to seek *authorisations* under the 2000 Act for directed or intrusive surveillance operations outside the UK only if the subject of investigation is a UK national or is likely to become the subject of criminal proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court.

1.23. *Authorisations* under Part II of the 2000 Act will be required in relation to overseas conduct principally in those circumstances where the conduct would otherwise be unlawful by virtue of the Human Rights Act 1998. *Authorisations* under the 2000 Act will usually therefore be appropriate for all directed and intrusive surveillance operations occurring in UK Embassies, military bases and detention facilities.

1.24. Under the provisions of section 76A of the 2000 Act, as inserted by the Crime (International Co-Operation) Act 2003, **foreign surveillance teams** may operate in the UK subject to certain conditions. See Chapter 5 (Authorisation procedures for directed surveillance) for detail.

8 or proceedings before an officer in respect of a service offence within the meaning of the Armed Forces Act 2006.

2. Directed and intrusive surveillance definitions

2.1. This chapter provides further guidance on whether covert surveillance activity is **directed surveillance, intrusive surveillance**, where an **authorisation for either activity** may not be required under Part II of the 2000 Act.

Directed surveillance

2.2. Surveillance is **directed surveillance** if the following are all true:

- it is **covert**, but not intrusive surveillance;
- it is conducted for the purposes of a **specific investigation or operation**;
- it is likely to result in the obtaining of *private information* about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- it is conducted **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* under Part II of the 2000 Act to be sought.

2.3. Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of *private information* about that, or any other person.

Private information

2.4. The 2000 Act states that *private information* includes any information relating to a person's **private or family life**[9]. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family[10] and professional or business relationships.

2.5. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of *private information*. This is **likely** to be the case where that person has a **reasonable expectation of privacy** even though acting in public and where a **record** is being made by a *public authority* of that person's activities for future consideration or analysis[11].

Example: *Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation and otherwise than by way of an immediate response to events.*

2.6. Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or some cases overtly) obtained for purposes of making a permanent record on that person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes surveillance, a directed surveillance authorisation may be required.

9 See section 26(10) of the 2000 Act.
10 Family should be treated as extending beyond the formal relationships created by marriage or civil partnership.
11 Note also that a person in police custody will have certain expectations of privacy.

Example: *Officers of a local authority wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the authority wished to conduct a similar exercise several times, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person or persons and a directed surveillance authorisation should be considered*

2.7. *Private information* may include personal data, such as name, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance *authorisation* is appropriate[12].

Example: *A Surveillance officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation. Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A directed surveillance authorisation should therefore be sought.*

Specific situations requiring directed surveillance authorisations

2.8. The following specific situations may also constitute directed surveillance according to the 2000 Act and a Part II authorisation should therefore be sought::

- **Surveillance devices** designed or adapted for the purpose of providing information regarding the **location of a vehicle** alone do not necessarily constitute directed surveillance if no private information about any individual is obtained but only information about the location of that particular device at any one time. However, the subsequent use of that information coupled with other surveillance activity which may obtain private information, could interfere with Article 8 rights.[13];
- surveillance consisting in the **interception of a communication** in the course of its transmission by means of a public postal service or telecommunication system where the communication is one sent or intended for a person who has **consented** to the interception of communications sent by or to him and where there is no interception *warrant*[14] authorising the interception[15].

Recording of telephone conversations

2.9. Subject to paragraph 2.8 above, the warranted interception of communications in the course of their transmission by means of a postal service or a telecommunications system may be authorised only by the *Secretary of State*, in accordance with the terms of Part I of the 2000 Act. Nothing in this code should be taken as granting dispensation from the requirements of that Part of the 2000 Act.

2.10. The recording or monitoring of one or both ends of a telephone conversation by a surveillance device as part of an authorised directed (or intrusive) surveillance operation will not constitute interception under Part I of the 2000 Act provided the process by which the content of the communication is obtained during the course of its transmission does not involve any modification of, or interference with, the telecommunications system or its operation. A telecommunications system begins at the point at which the sound waves representing the conversation reach the telephone handset and are converted to an electrical impulse or signal for onward transmission through the system. The recording or monitoring of one or both ends of a telephone conversation by a surveillance device will not therefore constitute interception as sound waves obtained from the air are not

12 There may of course be other lawful means of obtaining personal data which do not involve directed surveillance and which do not therefore require a directed surveillance authorisation under Part II of the 2000 Act.

13 This may also require an authorisation for property interference under the 1994 or 1997 Act. See Chapter 7

14 i.e. under Part 1 Chapter 1 of the 2000 Act

15 See section 48(4) of the 2000 Act. The availability of a directed surveillance authorisation nevertheless does not preclude authorities from seeking an interception *warrant* under Part I of the 2000 Act in these circumstances.

in the course of transmission by means of a telecommunications system (which, in the case of a telephone conversation, should be taken to begin with the microphone and end with the speaker). Any such product can be treated as having been lawfully obtained.

Example: *A property interference authorisation may be used to authorise the installation in a private car of an eavesdropping device with a microphone, together with an intrusive surveillance authorisation to record or monitor speech within that car. If one or both ends of a telephone conversation held in that car are also recorded during the course of the operation, this will not constitute unlawful interception provided the device obtains the product from the sound waves in the vehicle and not by interference with, or modification of, any part of the telecommunications system.*

Intrusive surveillance

[The references in the following passage to surveillance of legal consultations reflect the content of a statutory instrument under s. 47 RIPA which the Home Secretary intends to bring before Parliament, subject to the outcome of this consultation.]

2.11. **Intrusive surveillance** is **covert surveillance** that is carried out in relation to anything taking place on **residential premises** or in any **private vehicle** (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device. Covert surveillance is intrusive in these locations whether or not the activity subject to surveillance relates to the resident of the premises or owner of the vehicle. Directed surveillance that is carried out in relation to anything taking place on any premises where it is known that communications subject to legal privilege are being made must also be treated for the purposes of Part II as intrusive surveillance.

2.12. The definition of surveillance as intrusive relates to the **location** of the subject of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained. It is assumed that any information obtained from such locations is likely to be of a private or confidential nature.

Residential premises

2.13. For the purposes of the 2000 Act, **residential premises** are considered to be so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. This specifically includes hotel or prison accommodation that is so occupied or used[16]. However, **common areas** (such as hotel dining areas) to which a person has access in connection with their use or occupation of accommodation are specifically excluded[17].

2.14. The 2000 Act further states that the concept of premises should be taken to include any place whatsoever, including any vehicle or moveable structure, whether or not occupied as land.

2.15. Examples of residential premises would therefore include:

- a rented flat currently occupied for residential purposes;
- a prison cell (or police cell serving as temporary prison accommodation);
- a hotel bedroom or suite;
- a lorry cab used to sleep overnight (although not regarded as a dwelling for the purpose of property interference).

2.16. Examples of premises which would **not** be residential would include:

- a communal stairway in a block of flats (unless known to be used as a temporary place of abode by, for example, a homeless person);
- a prison canteen or police interview room;

16 See section 48(1) of the 2000 Act
17 See section 48(7) of the 2000 Act

- a hotel reception area or dining room;.
- the front garden or driveway of premises readily visible to the public;
- residential premises occupied by a public authority for non-residential purposes, for example trading standards 'house of horrors' situations or undercover operational premises.

Private vehicles

2.17. A **private vehicle** is defined in the 2000 Act as **any vehicle**, including vessels, aircraft or hovercraft, which is used **primarily** for the **private purposes** of the person who owns it or a person otherwise having the right to use it. This would include, for example a company car, owned by a leasing company and used for business and pleasure by the employee of a company[18].

Places for Legal Consultations

2.18. **Premises where it is known that communications subject to legal privilege may take place** include the offices of barristers, solicitors or other recognised legal representatives, rooms specifically allocated in courts, police stations and prisons for conducting legal consultations or any other room or location temporarily provided for such purposes.

Further considerations

2.19. Intrusive surveillance may take place by means of a **person** or **device** located in the residential premises or private vehicle. Surveillance may also be intrusive if it is carried out by means of a device placed outside the premises or vehicle if the device consistently provides information of **the same quality and detail** as might be expected to be obtained from a device inside.[19]

Example: *An observation post outside residential premises which provides a limited view compared to that which would be achievable from within the premises does not constitute intrusive surveillance. However, a zoom lens, for example, which consistently achieves imagery of the same quality as that which would be visible from within the premises, would constitute intrusive surveillance.*

2.20. The use of a device for the purpose of providing information about the **location** of any private vehicle is not considered to be intrusive surveillance.[20] Such use may, however, be authorised as **directed surveillance**, where the recording and subsequent use of the information would amount to the covert monitoring of the movements of the occupant(s) of that vehicle. A property interference authorisation may also be required for the covert installation or deployment of the device.

Where authorisation is not required

2.21. Some covert surveillance activity does not constitute intrusive or directed surveillance for the purposes of Part II of the 2000 Act and no directed or intrusive surveillance *authorisation* can therefore be granted. Such activity includes:

- covert surveillance by way of an **immediate response** to events;
- covert surveillance as part of **general observation activities**;
- covert surveillance not **for the purposes of a specific investigation or a specific operation**;
- overt use of **CCTV and ANPR systems**;
- certain other **specific situations**.

18 See section 48(1) and 48 (7) of the 2000 Act
19 See section 26(5) of the 2000 Act.
20 See section 26(4) of the 2000 Act

2.22. Each situation is detailed and illustrated below.

Immediate response

2.23. Covert surveillance that is likely to reveal *private information* about a person but is carried out by way of an immediate response to sudden and unforeseeable events, such that it is not reasonably practicable to obtain an *authorisation* under the 2000 Act, does not require a directed surveillance *authorisation*.

Example: *An authorisation under the 2000 Act is not available where police officers conceal themselves to observe suspicious persons that they come across in the course of a routine patrol.*

General observation activities

2.24. The general observation duties of many law enforcement officers and other *public authorities* do not require *authorisation* under 2000 Act, whether covert or overt. Such general observation duties frequently form part of the statutory functions of *public authorities* against breaches of law and order, as opposed to the pre-planned surveillance of a specific person or group of people. Wherever these activities are unlikely to result in the obtaining of *private information* about a person no directed surveillance *authorisation* is available.

Example 1: *Plain clothes police officers on patrol to monitor a high street crime hot-spot or prevent and detect shoplifting would not require a directed surveillance authorisation. Their objective is merely to observe a location and to identify and arrest offenders committing crime. The activity may be part of a specific investigation but is general observational activity, rather than surveillance and the obtaining of private information is unlikely. A directed surveillance authorisation is not available.*

Example 2: *Local authority officers monitoring a car boot sale where it is suspected that counterfeit goods are being sold. Again this is part of the general duties of public authorities and the likelihood of obtaining private information about any person is negligible.*

Example 3: *Surveillance officers intend to follow and observe Z covertly as part of a pre-planned operation to determine their suspected involvement in shoplifting. It is proposed to conduct covert surveillance of Z and record their activities as part of the investigation. In this case, private life considerations are likely to arise and a directed surveillance authorisation should be sought.*

Not for the purposes of a specific investigation or a specific operation

2.25. An *authorisation* for directed surveillance is not available if the surveillance is undertaken other than for the purposes of a "specific investigation or a specific operation." Covert surveillance for any other general purposes should be conducted under other legislation.

2.26. Directed surveillance is carried out by public authorities which are responsible for the discharge of specific public functions and are equipped with investigatory powers for the performance of those functions. In C v The Police and the Secretary of State for the Home Office - IPT/03/32/H dated 14 November 2006) the Investigatory Powers Tribunal held that directed surveillance under Part II is limited:

". . . to the discharge of the public authority's particular public or "core function" specific to it, rather than the carrying out of "ordinary functions" common to all public authorities, such as employment (or its nearest equivalent in the case of the police) and entering into contracts to receive or supply other services."

2.27. In practice, this means that a Part II authorisation is only available in respect of the carrying out of the 'specific public functions' undertaken by a particular authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc). The disciplining of an employee is not usually a 'core function', although it may be if it relates to a criminal offence. For example, if an employee was suspected by his public authority employer of criminal activities in the course of his work which would endanger national security or involve threats to public order then a Part II directed surveillance authorisation may be available.

Example: *A police officer is suspected by their employer of undertaking additional employment in breach of discipline regulations. The police force of which he is a member wishes to conduct covert surveillance of the officer outside the police work environment. Such activity, even if it is likely to result in the obtaining of private information, does not constitute directed surveillance for the purposes of the 2000 Act as it does not relate to the discharge of the police force's core functions and is not therefore being undertaken for the purposes of a "specific investigation or a specific operation". It relates instead to the carrying out of ordinary functions, such as employment, which are common to all public authorities. Activities of this nature are covered by the Data Protection Act 1998 and employment practices code.*

CCTV and ANPR (Automatic Number Plate Recognition) systems

2.28. The use of overt CCTV systems by *public authorities* does not require an *authorisation* under the 2000 Act. Members of the public will be aware that such systems are in use [21], and their operation is covered by the Data Protection Act 1998 and the CCTV Code of Practice 2008. Similarly, the use of ANPR systems to monitor traffic flows or detect motoring offences does not require an *authorisation* under the 2000 Act. The use of ANPR is this manner will obtain personal data through the capture of the vehicle registration number but the use of such systems is also conducted in accordance with the framework of the Data Protection Act 1998.

Example: *There may be circumstances where overt surveillance equipment, such as town centre closed-circuit television (CCTV) systems or ANPR, is used to gather information as part of a reactive operation (eg, attempts to identify offenders for criminal damage offences in a town centre or disqualified drivers). This may not necessarily amount to covert surveillance if the persons subject to the surveillance are aware that it is taking place. Use in these circumstances is unlikely to interfere with Article 8 rights under the ECHR and is generally no more than an intelligence driven use of the crime prevention and detection capability of CCTV or ANPR.*

2.29. However, where CCTV or ANPR systems are used in a covert and pre-planned manner for the surveillance of a specific person or group of people, a directed surveillance *authorisation* should be sought. Such covert surveillance forms part of a specific investigation or operation and may result in the obtaining of *private information* about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance. The use of the CCTV or ANPR system in these circumstances goes beyond their intended use for the general prevention and detection of crime and protection of the public.

Example: *A local police team receive information that an individual suspected of committing thefts from motor vehicles is known to be in a town centre area. A decision is taken to use the town centre CCTV system to conduct surveillance against that individual such that he remains unaware that there may be any specific interest in him. This targeted, covert use of the overt town centre CCTV system to monitor and/or record that individual's movements should be the subject of a directed surveillance authorisation.*

Specific situations not requiring directed surveillance authorisation

2.30. The following specific activities also constitute neither directed nor intrusive surveillance and therefore an *authorisation* under the 2000 Act cannot be granted:

- the use of a **recording device** by a **covert human intelligence source** who has been properly tasked to record any information which is disclosed in his presence;[22]
- the use of apparatus outside any residential or other premises exclusively for the purpose of **detecting the installation or use of a television receiver** within those premises;[23]

21 For example, by virtue of cameras or signage being clearly visible. See the CCTV Code of Practice 2008 for full guidance on establishing and operating overt CCTV systems.

22 See section 48(3) of the 2000 Act

23 See section 26(6) of the 2000 Act

- entry on or interference with property or wireless telegraphy which would be unlawful unless authorised under section 5 of the 1994 Act or Part III of the 1997 Act (such activity may be conducted in support of surveillance, but is not in itself surveillance).[24]

24 See section 48(3) of the 2000 Act

3. General rules on authorisations

Overview

3.1. An *authorisation* under Part II of the 2000 Act will, providing the statutory tests are met, provide a lawful basis for a *public authority* to carry out covert surveillance activity that is likely to result in the obtaining of *private information* about a person. Similarly, an *authorisation* under section 5 of the 1994 Act or Part III of the 1997 Act will provide lawful authority for *members* of the intelligence services, police, SOCA, SCDEA or HMRC to enter on, or interfere with, property or wireless telegraphy.

3.2. Responsibility for granting *authorisations* varies depending on the nature of the operation and the *public authority* involved. The relevant *public authorities* and *authorising officers* are detailed in…[Consolidating Order].

Necessity and proportionality

3.3. The 2000 Act, 1997 Act and 1994 Act stipulate that the person granting an *authorisation* or *warrant* for directed or intrusive surveillance, or interference with property, must believe that the activities to be authorised are **necessary** on one or more statutory grounds.[25]

3.4. If the activities are deemed necessary on one of more of the statutory grounds, the person granting the *authorisation* or *warrant* must also believe that they are **proportionate** to what is sought to be achieved by carrying them out. 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.

3.5. The *authorisation* will not be proportionate if it is excessive in the overall circumstances of the case. Each action to be conducted 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 be **reasonably obtained by other less intrusive means**. In general, the interferences that result from the carrying out of directed surveillance are likely in general to be less serious, in ECHR terms, than those that result from intrusive surveillance.

3.6. The following points should therefore be addressed when considering whether the authorised conduct is proportionate to what is sought to be achieved by carrying it out:

- the extent of the interference with privacy to which the proposed activity is likely to give rise when balanced against the strength and importance of the public policy justification in issue;
- how and why the methods to be adopted will impair as little as possible the rights in question;
- that the activity is rational and appropriate in all the circumstances and, having considered all possible courses of action, is no more than is necessary to accomplish the objective.

3.7. It is important therefore that all those involved in undertaking directed or intrusive surveillance activities or interference with property under the 2000 Act, 1997 Act or 1994 Act are fully aware of the extent and limits of the *authorisation* or *warrant* in question.

25 These statutory grounds are laid out in sections 28(3) of the 2000 Act for directed surveillance; section 32(3) of the 2000 Act for intrusive surveillance; and section 93(2) of the 1997 Act and section 5 of the 1994 Act for property interference. They are detailed in Chapters 5, 6 and 7 for directed surveillance, intrusive surveillance and interference with property respectively.

Example 1: *An individual is suspected of carrying out a series of minor criminal damage offences at a local shop following a dispute with the owner. It is suggested that a period of directed surveillance should be conducted to record the individual's movements and activities on the basis that the authorisation is necessary for the purpose of preventing or detecting crime. Although preventing and detecting crime is, in principle, a legitimate ground on which a directed surveillance authorisation may be granted, it is unlikely that the resulting interference with privacy will be necessary or proportionate in the circumstances of the particular case. In particular, the obtaining of private information on the individual's daily routine [and potentially that of innocent third parties with whom he associates] is unlikely to be required in order to investigate the activity of concern. Instead, other less intrusive means are likely to be available, such as general observation of the location in question until such time as a crime may be committed (see earlier example, paragraph 2.25)*

Example 2: *An individual is suspected of fabricating a false address within the catchment area of a particular school in order to abuse a school admissions system operated by the local education authority. The local authority believes a directed surveillance authorisation is necessary to investigate the individual for the purpose of preventing or detecting crime (in this case, fraud). Although these would be legitimate grounds for seeking a directed surveillance authorisation, such surveillance will not be necessary or proportionate to investigate the activity. Instead, it is likely that other less intrusive, and overt, means (such as unscheduled visits to the address in question) could be explored to obtain the required information.*

Example 3: *An individual is suspected of a relatively minor offence, such as littering, leaving waste out for collection unduly early, or permitting dog-fouling in a public place. It is suggested that a directed surveillance authorisation should be obtained in order to record his movements and activities for the purpose (as relevant) of preventing or detecting crime or protecting public health. Although these are legitimate grounds on which a directed surveillance authorisation may be granted, the tests of necessity and proportionality will not be satisfied in the circumstances of this particular case and the nature of the surveillance to be conducted. In particular, the obtaining of private information on the individual's daily routine and potentially of innocent third parties with whom he associates is unlikely to be required in order to investigate the activity of concern. Instead, readily available and less intrusive measures should be considered, such as general observation of the location in question until such time as a crime may be committed (see earlier example, paragraph 2.25). In addition, it is likely that such or offences can be tackled using overt techniques.*

Collateral intrusion

3.8. Before authorising *applications* for directed or intrusive surveillance, the *authorising officer* should also take into account the risk of obtaining *private information* about persons who are **not** subjects of the surveillance or property interference activity (collateral intrusion).

3.9. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion.

3.10. All *applications* should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the *authorising officer* fully to consider the proportionality of the proposed actions.

Example: *HMRC seeks to conduct directed surveillance against T on the grounds that this is necessary and proportionate for the collection of a tax. It is assessed that such surveillance will unavoidably result in the obtaining of some information about members of T's family, who are not the intended subjects of the surveillance. The authorising officer should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the authorisation. This may include not recording or retaining any material obtained through such intrusion.*

3.11. Note that where it is proposed to conduct surveillance activity or property interference specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion

but rather as intended intrusion. Any such surveillance or property interference activity should be carefully considered against the necessity and proportionality criteria as described above (paragraphs 3.3-3.8).

Example: *A law enforcement agency seeks to conduct a covert surveillance operation to establish the whereabouts of N in the interests of preventing a serious crime. It is proposed to conduct directed surveillance against P, who is an associate of N but who is not assessed to be involved in the crime, in order to establish the location of N. In this situation, P will be the subject of the directed surveillance authorisation and the authorising officer should consider the necessity and proportionality of conducting directed surveillance against P, bearing in mind the availability of any other less intrusive means to identify N's whereabouts. It may be the case that directed surveillance of P will also result in obtaining information about P's family, which in this instance would represent collateral intrusion also to be considered by the authorising officer.*

Combined authorisations

3.12. A single authorisation may combine:

- any number of *authorisations* under Part II of the 2000 Act; [26]
- an *authorisation* under Part II of the 2000 Act[27] and an *authorisation* under Part III of the 1997 Act;
- a warrant for intrusive surveillance under Part II of the 2000 Act[28] and a warrant under section 5 of the 1994 Act.

3.13. For example, a single *authorisation* may combine *authorisations* for directed and intrusive surveillance. However, the provisions applicable for each of the *authorisations* must be considered separately by the appropriate authorising officer. Thus, a police superintendent could authorise the directed surveillance element but the intrusive surveillance element would need the separate *authorisation* of a of a chief constable and the approval of a Surveillance Commissioner, unless the case is urgent.

3.14. The above considerations do not preclude *public authorities* from obtaining separate *authorisations*.

Collaborative working

3.15. Any person granting or applying for an *authorisation* will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of any similar activities being undertaken by other *public authorities* which could impact on the deployment of surveillance. It is therefore recommended that where an *authorising officer* from a *public authority* considers that conflicts might arise they should consult a senior officer within the police force area in which the investigation or operation is to take place.

3.16. In cases where one agency or force is acting on behalf of another, the tasking agency should normally obtain or provide the *authorisation* under Part II of the 2000 Act. For example, where surveillance is carried out by the police on behalf of HMRC, *authorisations* would usually be sought by HMRC and granted by the appropriate *authorising officer*. Where the operational support of other agencies (in this example, the police) is foreseen, this should be specified in the *authorisation*.

3.17. Where possible, *public authorities* should seek to avoid duplication of *authorisations* as part of a single investigation or operation. For example, where two agencies are conducting directed or intrusive surveillance as part of a joint operation, only one *authorisation* is required. Duplication of *authorisations* does not affect the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on authorities.

[The following provisions are subject to changes contained in the Policing and Crime Bill currently before Parliament:]

26 see section 43(2) of the 2000 Act

27 on the application of a *member* of a police force, SOCA, a customs officer or an officer of the OFT. See section 33(5) of the 2000 Act

28 on the application of a *member* of the intelligence services. See section 42(2) of the 2000 Act

3.18. Further, subject to paragraph 3.19 below:

- police, SOCA and HMRC *applications* for **directed surveillance** or **intrusive surveillance**, and OFT *applications* for **intrusive surveillance**, must only be made by a *member* or *officer* of the same force or agency as the *authorising officer*, regardless of which force or agency is to conduct the activity;
- *authorisations* for **intrusive surveillance** relating to **residential premises** may only authorise conduct where those premises are in the **same regional area** of operation of the force or agency applying for the *authorisation*.

3.19. With regard to police forces maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London), the Metropolitan police force and the City of London police force, the restrictions outlined in paragraph 3.18 may be varied in accordance with collaboration agreements made under section 23 of the Police Act 1996. With regard to police forces maintained under section 1 of the Police (Scotland) Act 1967, the restrictions in paragraph 3.18 may be varied in accordance with collaboration agreements made under section 12 of the Police (Scotland) Act 1967.]

Reviewing authorisations

3.20. Regular reviews of all authorisations should be undertaken to assess the need for the surveillance or property interference activity to continue. The results of a review should be retained for at least three years (see Chapter 8). Particular attention is drawn to the need to review authorisations frequently where the surveillance or property interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

3.21. In each case the frequency of reviews should be considered at the outset by the *authorising officer* or, for those subject to authorisation by the *Secretary of State*, the *member* or *officer* who made the *application* within the *public authority* concerned. This should be as frequently as is considered necessary and practicable.

3.22. In some cases it may be appropriate for an *authorising officer* to delegate the responsibility for conducting any reviews to a subordinate officer. The Authorising Officer is, however, usually best placed to assess whether the authorisation should continue or whether the criteria on which he based the original decision have changed sufficiently to cause a revocation of the authorisation. Support staff can do the necessary research and prepare the review process but the actual review is the responsibility of the original Authorising Officer and should, as a matter of good practice, be conducted by them or, failing that, by an officer who would be entitled to grant a new authorisation in the same terms.

3.23. Any proposed or unforeseen changes to the nature or extent of the surveillance operation that may result in further or greater intrusion into the private life of any person should also be brought to the attention of the authorising officer by means of a review. The authorising officer should consider whether the proposed changes are proportionate (bearing in mind any extra intended intrusion into privacy or collateral intrusion), before approving or rejecting them. Any such changes must be highlighted at the next renewal if the authorisation is to be renewed.

3.24. Where a directed or intrusive surveillance *authorisation* provides for the surveillance of unidentified individuals whose identity is later established, the terms of the *authorisation* should be refined at a review to include the identity of these individuals. It would be appropriate to convene such a review specifically for this purpose. This process will not require a fresh *authorisation*, providing the scope of the original authorisation envisaged surveillance of such individuals. Such changes must be highlighted at the next renewal if the *authorisation* is to be renewed.

Example: *A directed surveillance authorisation is obtained by the police to authorise surveillance of "X and his associates" for the purposes of investigating their suspected involvement in a crime. X is seen meeting with A in a café and it is assessed that subsequent surveillance of A will assist the investigation. Surveillance of A may continue (he is an associate of X) but the directed surveillance authorisation should be amended at a review to include "X and his associates, including A."*

General best practice

3.25. The following are not statutory requirements or formal provisions of this code, but should be considered as best working practices by all *public authorities* with regard to all *applications* for *authorisations* covered by this code:

- a*pplications* should avoid any repetition of information;
- information contained in a*pplications* should be limited to that required by the relevant legislation[29];
- where *authorisations* are granted orally under urgency procedures (see Chapters 5, 6 and 7 on authorisation procedures), a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the *applicant* and *authorising officer* as a priority. There is then no requirement subsequently to submit a full written *application*;
- an *application* should not require the sanction of any person in a *public authority* other than the *authorising officer*;
- where it is foreseen that other agencies will be involved in carrying out the surveillance, these agencies should be detailed in the *application*;
- *authorisations* should not generally be sought for activities already authorised following an application by the same or different *public authority*.

3.26. Furthermore, it is considered good practice that within every relevant *public authority,* a senior officer[30] should be responsible for:

- the integrity of the process in place within the *public authority* to authorise directed and intrusive surveillance and interference with property or wireless telegraphy;
- compliance with Part II of the 2000 Act, Part III of the 1997 Act and with this code;
- engagement with the Commissioners and inspectors when they conduct their inspections, and
- where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

29 As laid out in Chapters 5, 6 and 7 of this code

30 The senior responsible officer should be a person holding the office, rank or position of an *authorising officer* within the relevant public *authority*.

4. Confidential, legally privileged or Parliamentary information

Overview

4.1. The 2000 Act does not provide any special protection for '*confidential information*' although 1997 Act makes special provision for certain categories of confidential information. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where *confidential information* is involved. *Confidential information* consists of matters subject to **legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information,** or **confidential journalistic material**. So, for example, extra care should be taken where, through the use of surveillance, it is likely that knowledge will be acquired of communications between a minister of religion and an individual relating to the latter's spiritual welfare, or between a *Member* of Parliament and a constituent relating to constituency matters, or wherever matters of medical or journalistic confidentiality or *legal privilege* may be involved. Authorisations under the 1997 Act likely to result in the acquisition of knowledge of matters subject to legal privilege, confidential personal information or confidential journalistic material require (other than in urgent cases) the approval of a Surveillance Commissioner

4.2. References to a Member of Parliament include references to a Member of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

4.3. In cases where it is likely that knowledge of confidential information will be acquired, the use of covert surveillance is subject to a higher level of authorisation eg a Chief Officer [Consolidating order] lists the *authorising officer* for each *public authority* permitted to authorise such surveillance.

[The references in the following passage to surveillance of legal consultations reflect the content of a statutory instrument under s. 47 RIPA which the Home Secretary intends to bring before Parliament, subject to the outcome of this consultation.]

4.4. Directed surveillance is treated for the purposes of RIPA as intrusive surveillance where the surveillance takes place in locations where it is known that legal consultations are taking place. This means that, subject to paragraph 4.6 below, such surveillance cannot be undertaken without the prior approval of a Surveillance Commissioner (with the exception of *authorisations* requiring the approval of the *Secretary of State*). Such authorisations shall only be approved if the Commissioner is satisfied that there are reasonable grounds for believing that:

a) the authorisation is necessary in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom; and

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

4.5. Similarly, authorisation of action in respect of property in circumstances where it is believed that the action authorised is likely to result in the acquisition of knowledge of matters subject to legal privilege shall not be undertaken without the prior approval of a Surveillance Commissioner (with the exception of *authorisations* requiring the approval of the *Secretary of State*). Such authorisations shall only be approved if the Commissioner is satisfied that there are reasonable grounds for believing that:

a) the action specified is necessary to be taken for the purpose of preventing or detecting serious crime;

b) that the taking of the action is proportionate to what the action seeks to achieve.

4.6. With the exception of urgent *applications*, the *authorisation* for (as relevant) surveillance or action in respect

of property shall not take effect until such time as:

a) the *authorisation* has been approved by a Surveillance Commissioner; and

b) written notice of the Commissioner's decision to approve the *authorisation* has been given to the *authorising officer*.]

Communications subject to Legal Privilege

4.7. Section 98 of the 1997 Act describes those matters that are subject to *legal privilege* in England and Wales. In Scotland, the relevant description is contained in section 33 of the Criminal Law (Consolidation) (Scotland) Act 1995. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.

4.8. *Legal privilege* does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if there are grounds to believe, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose. But 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* applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

4.9. The 2000 Act does not provide any special protection for legally privileged information. Nevertheless, such information is particularly sensitive and surveillance which acquires such material may engage Article 6 of the ECHR (right to a fair trial) as well as Article 8. Legally privileged information obtained by surveillance is extremely unlikely ever to be admissible as evidence in criminal proceedings. Moreover, the mere fact that such surveillance has taken place may lead to any related criminal proceedings being stayed as an abuse of process. Accordingly, action which may lead to such information being acquired is subject to additional safeguards under this code.

4.10. In general, covert surveillance which is likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances. Full regard should be had to the particular proportionality issues such surveillance raises. The *application* should include, in addition to the reasons why it is considered necessary for the surveillance to take place, an assessment of how likely it is that information subject to *legal privilege* will be acquired. In addition, the *application* should clearly state whether the purpose (or one of the purposes) of the surveillance is to obtain legally privileged information.

4.11. This assessment will be taken into account by the *authorising officer* in deciding whether the proposed surveillance is necessary and proportionate under section 28 of the 2000 Act for directed surveillance and under section 32 for intrusive surveillance. The *authorising officer* or Surveillance Commissioner may require regular reporting so as to be able to decide whether the *authorisation* should continue. In those cases where legally privileged information has been acquired and retained, the matter should be reported to the *authorising officer* by means of a review and to the relevant Commissioner or Inspector during his next inspection (at which the material should be made available if requested).

4.12. A substantial proportion of the communications between a lawyer and his client(s) may be subject to *legal privilege*. Therefore, any case where a lawyer is the subject of an investigation or operation [will require the prior approval of a Surveillance Commissioner (with the exception of *authorisations* requiring the approval of the *Secretary of State*). Any material which has been retained from any such investigation or operation should be notified to the relevant Commissioner or Inspector during his next inspection and made available on request.]

4.13. Where there is any doubt as to the handling and dissemination of information which may be subject to *legal privilege,* advice should be sought from a legal adviser within the relevant *public authority* before any further dissemination of the material takes place. Similar advice should also be sought where there is doubt over whether information is not subject to *legal privilege* due to the "in furtherance of a criminal purpose" exception. The retention of legally privileged information, or its dissemination to an outside body, should be accompanied

by a clear warning that it is subject to *legal privilege*. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information. Any dissemination of legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

Communications involving Confidential Information

4.14. Similar consideration must also be given to *authorisations* that involve **confidential personal information, confidential constituent information** and **confidential journalistic material**. Where such material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested.

4.15. **Confidential personal information** is information held in confidence relating to the **physical or mental health** or **spiritual counselling** of a person (whether living or dead) who can be identified from it.[31] Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

4.16. **Confidential constituent information** is information relating to communications between a *Member* of Parliament and a constituent in respect of constituency matters. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

4.17. **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.

4.18. Where there is any doubt as to the handling and dissemination of **confidential information**, advice should be sought from a legal adviser within the relevant *public authority* before any further dissemination of the material takes place.

31 **Spiritual counselling** means conversations between a person and a religious authority acting in an official capacity, where the individual being counselled is seeking or the religious authority is imparting forgiveness, absolution or the resolution of conscience in accordance with their faith.

5. Authorisation procedures for directed surveillance

Authorisation criteria

5.1. Under section 28(3) of the 2000 Act an *authorisation* for directed surveillance may be granted by an *authorising officer* where he believes that the *authorisation* is necessary in the circumstances of the particular case on the grounds that it is:

a) in the interests of national security[32,33];

b) for the purpose of preventing or detecting[34] crime or of preventing disorder;

c) in the interests of the economic well-being of the UK;

d) in the interests of public safety;

e) for the purpose of protecting public health[35];

f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;[36] or

g) for any other purpose prescribed by an order made by the *Secretary of State*[37].

5.2. The *authorising officer* must also believe that the surveillance is proportionate to what it seeks to achieve (see 3.3-3.12).

Relevant public authorities

5.3. The *public authorities* entitled to authorise directed surveillance are listed in Schedule 1 to the 2000 Act. The specific purposes for which each *public authority* may obtain a directed surveillance *authorisation* are laid out in [Consolidated Order].

Authorisation procedures

5.4. Responsibility for authorising the carrying out of directed surveillance rests with the *authorising officer* and requires the personal authority of the *authorising officer*. The Regulation of Investigatory Powers (Prescriptions of Offices, Ranks and Positions) Order 2000; SI No: 2417 [*adjust to reflect consolidating order*] designates the *authorising* officer for each different *public authority* and the officers entitled to act in urgent cases. Where an *authorisation* for directed surveillance is combined with a *Secretary of State authorisation* for intrusive surveillance,

32 One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. An *authorising officer* in another *public authority* shall not issue a directed surveillance authorisation under Part II of the 2000 Act where the investigation or operation falls within the responsibilities of the Security Service, as set out above, except where the investigation or operation is to be carried out by a Special Branch or other police unit with formal counter-terrorism responsibilities (such as Counter Terrorism Units, Counter Terrorism Intelligence Units and Counter Terrorism Command) or where the Security Service has agreed that another *public authority* can carry out a directed surveillance investigation or operation which would fall within the responsibilities of the Security Service.

33 HM Forces may also undertake operations in connection with a military threat to national security and other operations in connection with national security in support of the Security Service, the Police Service of Northern Ireland or other Civil Powers.

34 Detecting crime is defined in section 81(5) of the 2000 Act and is applied to the 1997 Act by section 134 of that Act (as amended). Preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

35 This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

36 This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

37 This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

the combined authorisation must be issued by the *Secretary of State*.

5.5. The *authorising officer* must give authorisations in writing, except that in urgent cases, they may be given orally by the *authorising officer* or in writing by the officer entitled to act in urgent cases. In such cases, a record that the *authorising officer* has expressly authorised the action should be writing by both the authorising officer and the applicant as soon as is reasonably practical, together with the information detailed in paragraph 5.10 below.

5.6. 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 or applicant's* own making.

5.7. *Authorising officers* should not be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons. Where an *authorising officer authorises* such an investigation or operation the centrally retrievable record of authorisations (see Chapter 8) should highlight this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

5.8. *Authorising officers* within the Police and SOCA may only grant *authorisations* on application by a *member* of their own force or agency. [*Pending cross-authorisation developments.*] *Authorising officers* within HMRC may only grant *authorisations* on application by an *officer* of Revenue and Customs.

Information to be provided in applications for authorisation

5.9. A written *application* for a directed surveillance authorisation should describe any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- the reasons why the *authorisation* is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in Section 28(3) of the 2000 Act;
- the nature of the surveillance as defined at 1.9;
- the identities, where known, of those to be the subject of the surveillance;
- a summary of the intelligence case and appropriate unique intelligence references where applicable
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authorisation was given or refused, by whom and the time and date.

5.10. In urgent cases, the above information may be supplied orally. In such cases the authorising officer and applicant, where applicable, should also record the following information in writing, as soon as is reasonably practical (it is not necessary to record further detail):

- the identities of those subject to surveillance;
- he nature of the surveillance as defined at 1.9;
- the reasons why the *authorising officer* or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of a written *authorisation* was given; and/or

- the reasons why it was not reasonably practicable for the *application* to be considered by the *authorising officer*.

Where the officer entitled to act in urgent cases has given written authority, the reasons why it was not reasonably practicable for the *application* to be considered by the *authorising officer* should also be recorded.

Duration of authorisations

5.11. A written *authorisation* granted by an *authorising officer* will cease to have effect (unless renewed or cancelled) at the end of a period of **three months** beginning with the day on which it took effect. So an authorisation given at 09.00 on 12 February will expire on 11 May. (Authorisations (except those lasting for 72 hours) will cease at 23.59 on the last day).

5.12. Urgent oral *authorisations* or written *authorisations* granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after **seventy-two hours**, beginning with the time when the *authorisation* was granted.

Renewals

5.13. If, at any time before an *authorisation* for directed surveillance granted by a *member* of the intelligence services would cease to have effect, a *member* of the intelligence services who is entitled to grant such *authorisations* considers that it is necessary for the *authorisation* to continue on the on the grounds of **national security** or in the interests of the **economic well-being** of the UK, he may renew it for a further period of **six months**, beginning with the day on which it would have ceased to have effect but for the renewal.

5.14. If, at any time before any other directed surveillance *authorisation* would cease to have effect, the *authorising officer* considers it necessary for the *authorisation* to continue for the purpose for which it was given, he may renew it in writing for a further period of **three months**. Renewals may also be granted orally in urgent cases and last for a period of **seventy-two hours**. The renewal will take effect at the time at which, or day on which, the *authorisation* would have ceased to have effect but for the renewal.

5.15. An *application* for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new *authorisation* can renew an *authorisation*. *Authorisations* may be renewed more than once, provided they continue to meet the criteria for authorisation.

5.16. All *applications* for the renewal of a directed surveillance *authorisation* should record (at the time of application, or when reasonably practical in the case of urgent cases approved orally):

- whether this is the first renewal or every occasion on which the *authorisation* has been renewed previously;
- any significant changes to the information in paragraph 5.9;
- the reasons why the authorisation for directed surveillance should continue;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

5.17. *Authorisations* may be renewed more than once, if necessary, and the details of the renewal should be centrally recorded (see Chapter 8).

Cancellations

5.18. During a review, the *authorising officer* who granted or last renewed the *authorisation* may amend specific aspects of the authorisation, for example, to cease surveillance against one of a number of named subjects or to discontinue the use of a particular tactic. They must cancel the authorisation if satisfied that the directed surveillance as a whole no longer meets the criteria upon which it was authorised. Where the original *authorising officer* is no longer available, this duty will fall on the person who has taken over the role of *authorising officer*

or the person who is acting as *authorising officer* (see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794). [– adjust for Consolidating Orders]

5.19. As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date the *authorisation* was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained (see Chapter 8). There is no requirement for any further details to be recorded when cancelling a directed surveillance *authorisation* however effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

Foreign surveillance teams operating in UK

5.20. The provisions of section 76A of the 2000 Act as inserted by the Crime (International Co-Operation) Act 2003 provide for **foreign surveillance teams** to operate in the UK, subject to the following procedures and conditions.

5.21. Where a foreign police or customs officer[38], who is conducting directed or intrusive surveillance activity outside the UK , needs to enter the UK[39] for the purposes of continuing that surveillance, and where it is not reasonably practical for a United Kingdom officer[40] to carry out the surveillance under the authorisation of Part II of the 2000 Act (or RIP(S)A 2000), the foreign officer must notify a person designated by the Director General of SOCA immediately after entry to the UK and shall request (if this has not been done already) that an *application* for a directed surveillance *authorisation* be made under Part II of the 2000 Act (or RIP(S)A 2000).

5.22. The foreign officer may then continue to conduct surveillance for a period of five hours beginning with the time when the officer enters the UK. The foreign officer may only carry out the surveillance, however, in places to which *members* of the public are permitted access[41]. The directed surveillance *authorisation*, if obtained, will then authorise the foreign officers to conduct such surveillance beyond the five hour period in accordance with the general provisions of the 2000 Act.

38 as defined in section 76(A)(10) of the 2000 Act.

39 With the lawful authority of the country or territory in which it is being carried out and in respect of a suspected crime which falls within Article 40(7) of the Schengen Convention or which is a crime for the purposes of any other international agreement to which the United Kingdom is a party and which is specified for the purposes of section 76(A) of the 2000 Act in an order made by the *Secretary of State* with the consent of Scottish Ministers.

40 Being a *member* of a police force, SOCA, HMRC or a police *member* of the Scottish Crime and Drug Enforcement Agency appointed in accordance with paragraph 7 of schedule 2 to the Police, Public Order and Criminal Justice (Scotland) Act 2006 (asp 10)

41 whether on payment or otherwise.

6. Authorisation procedures for intrusive surveillance

General authorisation criteria

6.1. An *authorisation* for intrusive surveillance may be granted by the *Secretary of State* - for applications by the intelligence services, the Ministry of Defence or HM Forces[42] - or by a *senior authorising officer* or designated deputy of the police, SOCA, HMRC or OFT, as listed in section 32(6) and 34(6) of the 2000 Act.

6.2. In many cases, an investigation or operation using covert techniques may involve both intrusive surveillance and entry on, or interference with, property or with wireless telegraphy. In such cases, both activities need authorisation. This can be done as a combined *authorisation* (see paragraph 3.16).

6.3. Under section 32(2), (3) and (3A) of the 2000 Act the *Secretary of State* or the senior *authorising officer* or designated deputy may only authorise intrusive surveillance if they believe:

a) that the *authorisation* is necessary in the circumstances of the particular case on the grounds that it is:

- in the interests of national security [43];
- for the purpose of preventing or detecting[44] serious crime;
- in the interests of the economic well-being of the UK; or
- (in the case of the OFT) for the purpose of preventing or detecting an offence under section 188 of the Enterprise Act 2002 (cartel offence); and

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

6.4. When deciding whether an *authorisation* is necessary and proportionate, it is important to consider whether the information which it is thought necessary to obtain by means of the intrusive surveillance could reasonably be obtained by other less intrusive means.

Authorisations Procedures for the Police, SOCA, HMRC and OFT

Senior authorising officers and designated deputies

6.5. The **senior authorising officers** for these bodies are listed in section 32(6) of the 2000 Act. If the *senior authorising officer* is absent[45] then, under section 34(2) of the 2000 Act, an *authorisation* can be given by the **designated deputy** as provided for in section 12A of the Police Act 1996, section 5A of the Police (Scotland) Act 1967 and section 25 of the City of London Police Act 1839.

42 Or any other *public authority* designated for this purpose under section 41(1) of the 2000 Act.

43 A *senior authorising officer* or designated deputy of a law enforcement agency shall not issue an authorisation for intrusive surveillance where the investigation or operation is within the responsibilities of one of the intelligence services and properly falls to be authorised by *warrant* issued by the *Secretary of State* under Part II of the 2000 Act or the 1994 Act. See also notes 32, 42 and 53

44 See note 34

45 The consideration of an authorisation by the *senior authorising officer* is only to be regarded as not reasonably practicable (within the meaning of section 34(2) of the 2000 Act) if he is on annual leave, is absent from his office and his home, or is for some reason not able within a reasonable time to obtain access to a secure telephone or fax machine. Pressure of work is not normally to be regarded as rendering it impracticable for a *senior authorising officer* to consider an application. Where a designated deputy gives an authorisation this should be made clear and the reason for the absence of the *senior authorising officer* given.

Urgent cases

6.6. The *senior authorising* officer or designated deputy should generally give *authorisations* in writing. However, in urgent cases, oral *authorisations* may be given by the *senior authorising officer* or designated deputy. In an urgent oral case, a statement that the *senior authorising officer* or designated deputy has expressly authorised the conduct should be recorded in writing by the applicant as soon as is reasonably practical, together with the information detailed in paragraph 6.20 below.

6.7. In an urgent case, where it is not reasonably practicable having regard to the urgency of the case for either the *senior authorising officer* or the designated deputy to consider the *application*, an *authorisation* may be granted **in writing** by a person entitled to act only in urgent cases under section 34(4) of the 2000 Act.[46]

6.8. 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 generally to be regarded as urgent where the need for an *authorisation* has been neglected or the urgency is of the *authorising officer or applicant's* own making.

Jurisdictional considerations

6.9. A police or SOCA *authorisation* cannot be granted unless the *application* is made by a *member* of the same force or agency. [*Pending cross-authorisation developments.*] An HMRC or OFT *authorisation* cannot be granted unless the application is made by an *officer* of Revenue and Customs or OFT respectively.

6.10. Where the surveillance is carried out in relation to any residential premises, the *authorisation* cannot be granted unless the residential premises are in the **same area** of operation of the force or organisation.

Approval of Surveillance Commissioners

6.11. Except in urgent cases a police, SOCA, HMRC or OFT *authorisation* granted for intrusive surveillance will not take effect until it has been approved by a Surveillance Commissioner and written notice of the Commissioner's decision has been given to the person who granted the *authorisation*. This means that the approval will not take effect until the notice has been received in the office of the person who granted the *authorisation* within the relevant force or organisation.

6.12. When the *authorisation* is urgent it will take effect from the time it is granted provided notice is given to the Surveillance Commissioner in accordance with section 35(3)(b) (see section 36(3) of the 2000 Act).

6.13. There may be cases that become urgent after approval has been sought but before a response has been received from a Surveillance Commissioner. In such a case, the *authorising officer* should notify the Surveillance Commissioner that the case is now urgent (pointing out that it has become urgent since the notification). In these cases, the *authorisation* will take effect immediately.

Notifications to Surveillance Commissioners

6.14. Where a person grants, renews or cancels an *authorisation* for intrusive surveillance, he must, as soon as is reasonably practicable, give notice in writing to a Surveillance Commissioner, in accordance with whatever arrangements have been made by the Chief Surveillance Commissioner.[47]

6.15. In urgent cases, the notification must specify the grounds on which the case is believed to be one of urgency. The urgency provisions should not be used routinely. If the Surveillance Commissioner is satisfied that there were no grounds for believing the case to be one of urgency, he has the power to quash the *authorisation*.

46 Note that ACPO out-of-hours officers of assistant chief constable rank or above will be entitled to act for this purpose.

47 The information to be included in the notification to the Surveillance Commissioner is set out in the Regulation of Investigatory Powers (Notification of Authorisations etc.) Order 2000; SI No: 2563.

Authorisation Procedures for Secretary of State Authorisations

6.16. Intrusive surveillance by any of the intelligence services, the Ministry of Defence or HM Forces[48] requires the approval of a *Secretary of State*, unless these bodies are acting on behalf of another *public authority* that has obtained an *authorisation*.

6.17. Any *member* or official of the intelligence services, the Ministry of Defence and HM Forces can apply to the *Secretary of State* for an intrusive surveillance *authorisation*. *Applications* to the *Secretary of State* should specify those matters listed in paragraph 6.19 below.

6.18. Intelligence services *authorisations* must be made by issue of a *warrant*. Such *warrants* will generally be given in writing by the *Secretary of State*. In urgent cases, a *warrant* may be signed (but not renewed) by a senior official, with the express authorisation of the *Secretary of State*.

Information to be provided in all applications for intrusive surveillance

6.19. *Applications* should be in writing (unless urgent) and should describe the conduct to be authorised and the purpose of the investigation or operation. The *application* should specify:

- the reasons why the *authorisation* is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting serious crime) listed in section 32(3) of the 2000 Act;
- the nature of the surveillance as defined at 1.9;
- the residential premises or private vehicle in relation to which the surveillance will take place;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- details of any potential collateral intrusion and why the intrusion is justified;
- details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- a subsequent record should be made of whether authorisation was given or refused, by whom and the time and date.

6.20. In urgent cases, the above information may be supplied orally. In such cases the applicant should also record the following information in writing, as soon as is reasonably practical (it is not necessary to record further detail):

- the identities of those subject to surveillance;
- the nature and location of the surveillance;
- the reasons why the *authorising officer* or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of a written *authorisation* was given; and/or
- the reasons why it was not reasonably practicable for the *application* to be considered by the *authorising officer*.

Duration of intrusive surveillance authorisations

Secretary of State warrants for the intelligence services

6.21. A *warrant* issued by the *Secretary of State* will cease to have effect at the end of a period of **six months** beginning with the day on which it was issued. So an authorisation given at 09.00 on 12 February will expire

48 or any other *public authority* designated for this purpose under section 41(1) of the 2000 Act, such as the Home Office on the application of a *member* of HM Prison Service (SI 1126; 2001).

on 11 August. (Authorisations (except those granted under urgency provisions) will cease at 23.59 on the last day).

6.22. *Warrants* expressly authorised by a *Secretary of State*, but signed by a senior official under the urgency procedures, will cease to have effect at the end of the **second working day** following the day of issue of the *warrant* unless renewed by the *Secretary of State*.

All other intrusive surveillance authorisations

6.23. A written *authorisation* granted by a *Secretary of State*, a *senior authorising officer* or a designated deputy 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. So an authorisation given at 09.00 on 12 February will expire on 11 May. (Authorisations (except those lasting for 72 hours) will cease at 23.59 on the last day).

6.24. Oral *authorisations* given in urgent cases by a *Secretary of State*, a *senior authorising officer* or designated deputy, and written *authorisations* given by those only entitled to act in urgent cases (see paragraph 6.7), will cease to have effect (unless renewed) at the end of the period of **seventy-two hours** beginning with the time when they took effect.

Renewals of intrusive surveillance authorisations

Secretary of State authorisations

6.25. If at any time before an **intelligence service** *warrant* expires, the *Secretary of State* considers it necessary for the *warrant* to be renewed for the purpose for which it was issued, the *Secretary of State* may renew it in writing for a further period of **six months**, beginning with the day on which it would have ceased to have effect, but for the renewal.

6.26. If at any time before a *warrant* issued by a *Secretary of State* for any other *public authority* expires, the *Secretary of State* considers it necessary for the *warrant* to be renewed for the purpose for which it was issued, he may renew it in writing for a further period of **three months**, beginning with the day on which it would have ceased to have effect, but for the renewal.

All other intrusive surveillance authorisations

6.27. If, at any time before an *authorisation* expires, the *senior authorising officer* or, in his absence, the designated deputy considers that the *authorisation* should continue to have effect for the purpose for which it was issued, he may renew it in writing for a further period of **three months**.

6.28. As with the initial *authorisation*, the *senior authorising officer* must (unless it is a rare case to which the urgency procedure applies) seek the **approval of a Surveillance Commissioner**. The renewal will not take effect until the notice **of the Surveillance Commissioner's** approval has been received in the office of the person who granted the *authorisation* within the relevant force or organisation (but not before the day on which the *authorisation* would have otherwise ceased to have effect).

6.29. In urgent cases, a renewal can take effect immediately (provided this is not before the day on which the *authorisation* would have otherwise ceased to have effect). See section 35 and 36 of the 2000 Act and the Regulation of Investigatory Powers (Notification of Authorisations etc.) Order 2000; SI No: 2563.

Information to be provided for all renewals of intrusive surveillance authorisations

6.30. All *applications* for a renewal of an intrusive surveillance *authorisation* or warrant should record:

- whether this is the first renewal or every occasion on which the *warrant/authorisation* has been renewed previously;
- any significant changes to the information listed in paragraph 6.19;
- the reasons why it is necessary to continue with the intrusive surveillance;

- the content and value to the investigation or operation of the product so far obtained by the surveillance;
- the results of any reviews of the investigation or operation (see below).

6.31. *Authorisations* may be renewed more than once, if necessary, and details of the renewal should be centrally recorded (see Chapter 8).

Cancellations of intrusive surveillance activity

6.32. The *senior authorising officer* who granted or last renewed the authorisation must cancel it, or the person who made the *application* to the *Secretary of State* must apply for its cancellation, if he is satisfied that the surveillance no longer meets the criteria upon which it was authorised. Where the *senior authorising officer* or person who made the *application* to the *Secretary of State* is no longer available, this duty will fall on the person who has taken over the role of *senior authorising officer* or taken over from the person who made the *application* to the *Secretary of State* or the person who is acting as the senior *authorising officer*.[49]

6.33. As soon as the decision is taken that intrusive surveillance should be discontinued, the instruction must be given to those involved to stop the intrusive surveillance. The date the *authorisation* was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained (see Chapter 8). There is no requirement to record any further details however effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

6.34. Following the cancellation of any intrusive surveillance *authorisation*, other than one granted by the *Secretary of State*, the Surveillance Commissioners must be notified of the cancellation.[50]

Authorisations quashed by a Surveillance Commissioner

6.35. In cases where a police, SOCA, HMRC or OFT *authorisation* is quashed or cancelled by a Surveillance Commissioner, the *senior authorising officer* must immediately instruct those involved to stop carrying out the intrusive surveillance. Documentation of the date and time when such an instruction was given should be retained for at least three years (see Chapter 8).

49 See the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794.

50 This notification shall include the information specified in the Regulation of Investigatory Powers (Notification of Authorisations etc.) Order 2000; SI No: 2563.

7. Authorisation procedures for property interference

Appropriate authorisations

General basis for lawful activity

7.1. *Authorisations* under section 5 of the 1994 Act or Part III of the 1997 Act should be sought wherever *members* of the intelligence services, the police, the services police, Serious and Organised Crime Agency (SOCA), Scottish Crime and Drug Enforcement Agency (SCDEA), HM Revenue and Customs (HMRC) or Office of Fair Trading (OFT), or persons acting on their behalf, conduct entry on, or interference with, property or with wireless telegraphy that would be otherwise unlawful under existing legislation.[51]

7.2. For the purposes of this chapter, "property interference" shall be taken to include entry on, or interference with, property or with wireless telegraphy.

7.3. In many cases an operation using covert techniques may involve both directed or intrusive surveillance and property interference. This can be done as a combined *authorisation*, although the criteria for authorisation of each activity must be considered separately (see paragraph 3.17).

Example: *The use of a surveillance device for providing information about the location of a vehicle may involve some physical interference with that vehicle as well as subsequent directed surveillance activity. Such an operation could be authorised by a combined authorisation for property interference (under Part III of the 1997 Act) and, where appropriate, directed surveillance (under the 2000 Act). In this case, the necessity and proportionality of the property interference element of the authorisation would need to be considered by the appropriate authorising officer (see paragraph 7.9below).separately to the necessity and proportionality of obtaining private information by means of the directed surveillance.*

7.4. A Property Interference authorisation is not required for entry (whether for the purpose of covert recording or for any other legitimate purpose) into areas open to the public in shops, bars, restaurants, hotel foyers, blocks of flats or any other premises to which, with the implied consent of the occupier, members of the public are afforded unqualified access. Nor is authorisation required for entry on any other land or premises at the invitation of the occupier. This is so whatever the purposes for which the premises are used. If this consent for entry has been obtained by deception (e.g. requesting entry for a false purpose), it could be argued that this is not true consent and an authorisation for Property Interference should be obtained.

Informed consent

7.5. *Authorisations* under the 1994 Act and 1997 Act are not necessary where the *public authority* is acting with the informed consent of a person able to give permission in respect of the relevant property and actions. However, consideration should still be given to the need to obtain a directed or intrusive surveillance *authorisation* under Part II of the 2000 Act depending on the operation.

Example: *A vehicle is fitted with a security alarm to ensure the safety of an undercover officer. If the consent of the vehicle's owner is obtained to install this alarm, no authorisation under the 1997 Act is required. However, if the owner has not provided consent, an authorisation will be required to render lawful the property interference. The fact that the undercover officer is aware of the alarm installation is not relevant to the lawfulness of the property interference.*

51 Examples of such activity which may otherwise be unlawful include any access to or interference with computers that would be unlawful under the Computer Misuse Act 1990 and any misuse of wireless telegraphy apparatus as defined in the Wireless Telegraphy Act 2006.

Incidental property interference

7.6. The 2000 Act provides that no person shall be subject to any civil liability in respect of any conduct which is **incidental** to correctly authorised directed or intrusive surveillance activity **and** for which an *authorisation* or *warrant* is not capable of being granted or might not reasonably have been expected to have been sought under any existing legislation.[52] Thus a person shall not, for example, be subject to civil liability for trespass where that trespass is incidental to properly authorised directed or intrusive surveillance activity and where an *authorisation* under the 1994 Act or 1997 Act is available but might not reasonably have been expected to be sought (perhaps due to the unforeseeable nature or location of the activity).

7.7. Note that where an *authorisation* for the incidental conduct is not available (for example because the 1994 Act or 1997 Act do not apply to the public authority in question), the *public authority* shall not be subject to civil liability in relation to any incidental conduct, by virtue of section 27(2) of the 2000 Act. Note also however, that where a *public authority* is capable of obtaining an *authorisation* for the activity, it should seek one wherever it could be reasonably expected to do so.

7.8. Incidental conduct should be interpreted as that which is so closely connected to the surveillance, to the extent that the conduct is effectively unavoidable if the lawfully authorised surveillance is to take place.

Example: *Surveillance officers crossing an area of land covered by an authorisation under the 1997 Act are forced to temporarily and momentarily cross into neighbouring land to bypass an unforeseen obstruction, before returning to their authorised route.*

Samples

7.9. The acquisition of samples where there is no consequent loss of or damage to property (such as DNA samples, fingerprints and footwear impressions) does not of itself constitute unlawful property interference. However, wherever it is necessary to conduct otherwise unlawful property interference to access and obtain these samples, an *authorisation* under the 1994 or 1997 Act would be appropriate. An authorisation for directed or intrusive surveillance would not be available for any subsequent information, whether private or not, obtained as a result of the covert technique. In essence once a DNA sample, fingerprint or footwear impression has been obtained, any subsequent analysis of this information will not be surveillance as defined at s48(2). The appropriate lawful authority in these cases is likely to be the Data Protection Act.

Example: *Police wish to take fingerprints from a public telephone to identify a suspected criminal who is known recently to have used the telephone. The act of taking the fingerprints would not involve any unlawful property interference as the gathering of evidence in this case would be covered by PACE 84, so no authorisation under the 1994 or 1997 Act is required. The subsequent recording and analysis of the information obtained to establish the individual's identity would not amount to surveillance and therefore, would not require authorisation under the 2000 Act.*

Example: *Police intend covertly to acquire a mobile telephone used by a suspected criminal, in order to take fingerprints. In this case, the acquisition of the telephone for the purposes of obtaining fingerprints could be authorised under the 1994 or 1997 Act where it would otherwise be unlawful. Authorisation for directed surveillance would be appropriate if any further analysis of the mobile telephone, its stored contents or opening of incoming texts or messages is being considered.*

Authorisations for property interference by the police, the services police, SOCA, SCDEA, HMRC and OFT

7.10. Responsibility for these *authorisations* rests with the *authorising officer* as defined in section 93(5) of the 1997 Act, i.e. the chief constable or equivalent. *Authorisations* require the personal authority of the *authorising officer* (or his designated deputy) except in urgent situations, where it is not reasonably practicable for the *application* to be considered by such person. The person entitled to act in such cases is set out in section 94 of

52 See section 27(2) of the Act

the 1997 Act.

7.11. Any person giving an *authorisation* for entry on or interference with property or with wireless telegraphy under section 93(2) of the 1997 Act must believe that:

- it is necessary for the action specified to be taken for the purpose of preventing or detecting[53] serious crime[54,55] ; and
- that the taking of the action is proportionate to what the action seeks to achieve.

7.12. The *authorising officer* must take into account whether what it is thought necessary to achieve by the authorised conduct could reasonably be achieved by other means.

Collaborative working and regional considerations

7.13. *Authorisations* for the police, the military services police, SOCA, SCDEA, HMRC and OFT may only be given by an *authorising officer* on application by a *member* or *officer* of the same force or agency.

7.14. *Authorisations* for the police and SCDEA may only be given for property interference within the *authorising officer's* own area of operation. An *authorising officer* may authorise property interference (excluding wireless telegraphy interference) outside the relevant area solely for the purpose of maintaining (including replacing) or retrieving any device, apparatus or equipment the use of which within the relevant area has been authorised under the 1997 Act or 2000 Act. Authorisation for maintenance or retrieval outside of the authorising officer's own area of operations can only be given for circumstances that do not require entry onto private land.

7.15. Any person granting or applying for an *authorisation* or *warrant* to enter on or interfere with property or with wireless telegraphy will also need to be aware of particular sensitivities in the local community where the entry or interference is taking place and of similar activities being undertaken by other *public authorities* which could impact on the deployment. In this regard, it is recommended that the *authorising officers* in the services police, SOCA, SCDEA, HMRC and OFT should consult a senior officer within the police force in which the investigation or operation takes place where the *authorising officer* considers that conflicts might arise. The Chief Constable of the Police Service of Northern Ireland should be informed of any surveillance operation undertaken by another law enforcement agency which involves its officers maintaining (including replacing) or retrieving equipment in Northern Ireland.

Authorisation procedures

7.16. *Authorisations* will generally be given in writing by the *authorising officer*. However, in urgent cases, they may be given orally by the *authorising officer*. In such cases, a statement that the *authorising officer* has expressly authorised the action(s) should be recorded in writing by the applicant as soon as is reasonably practical, together with that information detailed in paragraph 7.19 below.

7.17. If the *authorising officer* is absent then an *authorisation* can be given in writing or, in urgent cases, orally by the designated deputy as provided for in section 94(4) of the 1997 Act, section 12(A) of the Police Act 1996, section 5(A) of the Police (Scotland) Act 1967, section 25 of the City of London Police Act 1839 or section 93(5) of the 1997 Act (for SOCA).

7.18. Where, however, in an urgent case, it is not reasonably practicable for the *authorising officer* or designated deputy to consider an *application,* then **written** *authorisation* may be given by the following:

53 see note 37

54 An *authorising officer* in a public authority other than the Security Service shall not issue an authorisation under Part III of the 1997 Act where the investigation or operation falls within the responsibilities of the Security Service. Where any doubt exists a *public authority* should confirm with the Security Service whether or not the investigation is judged to fall within Security Service responsibilities before seeking an authorisation under Part III of the 1997 Act. See also notes 32, 42 and 53

55 Where the *authorising officer* is the Chairman of the OFT, the only purpose falling within this definition is the purpose of preventing or detecting an offence under section 188 of the Enterprise Act 2002 (see section 93(2AA) of the 1997 Act

- in the case of the police, by an assistant chief constable (other than a designated deputy)[56];
- in the case of the Metropolitan Police and City of London Police, by a commander;
- in the case of MOD police or British Transport Police, by a deputy or assistant chief constable;
- in the case of the services police, by an assistant Provost Marshal (in the Royal Naval Police) or deputy Provost Marshal (in the Royal Military Police or Royal Air Force Police);
- in the case of SCDEA, by a chief constable, his designated deputy or an assistant chief constable;
- in the case of SOCA a person designated by the Director General;
- in the case of HMRC, by a person designated by the Commissioners of Revenue and Customs[57];
- in the case of the OFT, by an officer of the OFT designated for this purpose.

Information to be provided in applications

7.19. Applications to the *authorising officer* for the granting or renewal of an *authorisation* must be made in writing (unless urgent) by a police officer, Revenue and Customs officer[, SCDEA officer] or a member of SOCA (within the terms of SOCAP 2005) or an officer of the OFT and should specify:

- the identity or identities, where known, of those who possess the property that is to be subject to the interference;
- sufficient information to identify the property which the entry or interference with will affect;
- the nature and extent of the proposed interference;
- the details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why the intrusion is justified;
- details of the offence suspected or committed;
- how the authorisation criteria (as set out in paragraphs 7.10 and 7.11) have been met;
- any action which may be necessary to maintain (including replacing) any equipment;
- any action which may be necessary to retrieve any equipment;
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and
- whether an *authorisation* was given or refused, by whom and the time and date.

7.20. In urgent cases, the above information may be supplied orally. In such cases the *authorising officer* and the *applicant* should also record the following information in writing, as soon as is reasonably practical (it is not necessary to record further detail):

- the identity or identities of those owning or using the property (where known);
- sufficient information to identify the property which the entry or interference with will affect;
- details of the offence suspected or committed;
- the reasons why the *authorising officer* or designated deputy considered the case so urgent that an oral instead of a written *authorisation* was given; and/or
- the reasons why (if relevant) it was not reasonably practicable for the *application* to be considered by the *authorising officer* or the designated deputy.

56 ACPO out-of-hours officers of assistant chief constable rank or above will be entitled to act for this purpose.
57 This will be an officer of the rank of assistant chief investigation officer.

Notifications to Surveillance Commissioners

7.21. Where a person gives, renews or cancels an *authorisation* in respect of entry on or interference with property or with wireless telegraphy, he must, as soon as is reasonably practicable, give notice of it in writing to a Surveillance Commissioner, in accordance with arrangements made by the Chief Surveillance Commissioner. In urgent cases which would otherwise have required the approval of a Surveillance Commissioner, the notification must specify the grounds on which the case is believed to be one of urgency.

7.22. There may be cases which become urgent after approval has been sought but before a response has been received from a Surveillance Commissioner. In such a case, the *authorising officer* should notify the Surveillance Commissioner that the case is urgent (pointing out that it has become urgent since the previous notification). In these cases, the *authorisation* will take effect immediately.

7.23. Notifications to Surveillance Commissioners in relation to the granting, renewal and cancellation of *authorisations* in respect of entry on or interference with property should be in accordance with the requirements of the Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No. 3241.

Cases requiring prior approval of a Surveillance Commissioner

7.24. In certain cases, an *authorisation* for entry on or interference with property will not take effect until a Surveillance Commissioner has approved it and the notice of approval has been received in the office of the person who granted the *authorisation* within the relevant force or organisation (unless the urgency procedures are used). These are cases where the person giving the *authorisation* believes that:

- any of the property specified in the *authorisation*:

- is used wholly or mainly as a dwelling or as a bedroom in a hotel; or

- constitutes office premises[58]; or

- the action authorised is likely to result in any person acquiring knowledge of:

- matters subject to *legal privilege*;

- confidential personal information; or

- [*confidential constituent information; or*]

- confidential journalistic material.

Duration of authorisations

7.25. Written *authorisations*for entry on or interference with property will not take effect until a Surveillance Commissioner has approved it and the notice of approval has been received in the office of the person who granted the *authorising officers* will cease to have effect at the end of a period of **three months** beginning with the day on which they took effect. So an authorisation given at 09.00 on 12 February will expire on 11 May. (Authorisations (except those lasting for 72 hours) will cease at 23.59 on the last day).

7.26. In cases requiring prior approval by a Surveillance Commissioner (see paragraph 7.23) this means from the time at which the person who gave the *authorisation* was notified that the Surveillance Commissioner had approved the *authorisation*. This can be done by presenting the authorising officer with the approval decision page to note in person or if the authorising officer is unavailable, sending the written notice by auditable electronic means. In cases not requiring prior approval, this means from the time the *authorisation* was granted.

58 Office premises are defined as any building or part of a building whose sole or principal use is as an office or for office purposes (which means purposes of administration, clerical work, handling money and telephone or telegraph operation).

7.27. Oral *authorisations* given in urgent cases by:

- *authorising officers*
- or designated deputies
- and written *authorisations* given by the persons specified in 7.16 (section 94(3) of the 1997 Act)

will cease at the end of the period of **seventy-two** hours beginning with the time when they took effect.

Renewals

7.28. If at any time before the time and day on which an *authorisation* expires the *authorising officer* or, in his absence, the designated deputy considers the *authorisation* should continue to have effect for the purpose for which it was issued, he may renew it in writing for a period of three months beginning with the day on which the *authorisation* would otherwise have ceased to have effect. *Authorisations* may be renewed more than once, if necessary, and details of the renewal should be centrally recorded (see Chapter 8).

7.29. Commissioners must be notified of renewals of *authorisations*. The information to be included in the notification is set out in the Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No: 3241.

7.30. If, at the time of renewal, the criteria in paragraph 7.23 exist, then the approval of a Surveillance Commissioner must be sought before the renewal can take effect. The fact that the initial *authorisation* required the approval of a Commissioner before taking effect does not mean that its renewal will automatically require such approval. It will only do so if, at the time of the renewal, it falls into one of the categories requiring approval (and is not a rare urgent case).

Cancellations

7.31. The senior *authorising officer* who granted or last renewed the *authorisation* must cancel it if he is satisfied that the *authorisation* no longer meets the criteria upon which it was authorised. Where the *senior authorising officer* is no longer available, this duty will fall on the person who has taken over the role of *senior authorising officer* or the person who is acting as the senior authorising officer (see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794).

7.32. Following the cancellation of the *authorisation*, the Surveillance Commissioners must be notified of the cancellation. The information to be included in the notification is set out in the Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No: 3421.

7.33. The Surveillance Commissioners have the power to cancel an *authorisation* if they are satisfied that, at any time after an *authorisation* was given or renewed, there were no reasonable grounds for believing the matters set out in paragraphs 7.10 and 7.11 above. In such circumstances, a Surveillance Commissioner may order the destruction of records, in whole or in part, other than any that are required for pending criminal or civil proceedings.

Retrieval of equipment

7.34. Because of the time it can take to remove equipment from a person's property it may also be necessary to renew an *authorisation* in order to complete the retrieval. The notification to Commissioners of such a renewal should state why the operation is being or has been closed down, why it has not been possible to remove the equipment and, where possible, a timescale for removal.

7.35. Where a Surveillance Commissioner quashes or cancels an *authorisation* or renewal, he will, if there are reasonable grounds for doing so, order that the *authorisation* remain effective for a specified period, to enable officers to retrieve anything left on the property by virtue of the *authorisation*. He can only do so if the *authorisation* or renewal makes provision for this. A decision by the Surveillance Commissioner not to give such an order can be the subject of an appeal to the Chief Surveillance Commissioner.

Ceasing of entry on or interference with property or with wireless telegraphy

7.36. Once an *authorisation* or renewal expires or is cancelled or quashed, the *authorising officer* must immediately give an instruction to cease all the actions authorised for the entry on or interference with property or with wireless telegraphy. The time and date when such an instruction was given should be centrally retrievable for at least three years (see Chapter 8).

Authorisations for property interference by the intelligence services

7.37. An *application* for a *warrant* must be made by a *member* of the intelligence services for the taking of action in relation to that agency. In addition, the Security Service may make an *application* for a *warrant* to act on behalf of the Secret Intelligence Service (SIS) and the Governments Communication Headquarters (GCHQ). SIS and GCHQ may not be granted a warrant for action in support of the prevention and detection of serious crime which relates to property in the British Islands.

7.38. The intelligence services should provide the same information as other agencies (see paragraphs 7.18-7.19 above), as and where appropriate, when making *applications* for the grant or renewal of property *warrants*.

7.39. Before granting a warrant, the *Secretary of State* must:

- think it necessary for the action to be taken for the purpose of assisting the relevant agency in carrying out its functions;
- be satisfied that the taking of the action is proportionate to what the action seeks to achieve;
- take into account in deciding whether an *authorisation* is necessary and proportionate is whether the information which it is thought necessary to obtain by the conduct authorised by the *warrant* could reasonably be obtained by other means; and
- be satisfied that there are satisfactory arrangements in force under the 1994 Act or the 1989 Act in respect of disclosure of any material obtained by means of the *warrant*, and that material obtained will be subject to those arrangements.

Renewals of intelligence services warrants

7.40. A *warrant* shall, unless renewed, cease to have effect at the end of the period of **six months** beginning with the day on which it was issued (if the *warrant* was issued under the hand of the *Secretary of State*) or at the end of the period ending with the **fifth working day** following the day on which it was issued (in any other case).

7.41. If at any time before the day on which a *warrant* would cease to have effect the *Secretary of State* considers it necessary for the *warrant* to continue to have effect for the purpose for which it was issued, he may by an instrument under his hand renew it for a period of **six months** beginning with the day it would otherwise cease to have effect.

Cancellations of intelligence services warrants

7.42. The *Secretary of State* shall cancel a *warrant* if he is satisfied that the action authorised by it is no longer necessary.

7.43. The person who made the *application* to the *Secretary of State* must apply for its cancellation, if he is satisfied that the *warrant* no longer meets the criteria upon which it was authorised. Where the person who made the *application* to the *Secretary of State* is no longer available, this duty will fall on the person who has taken over from the person who made the *application* to the *Secretary of State* (see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794)

Retrieval of equipment by the intelligence services

7.44. Because of the time it can take to remove equipment from a person's property it may also be necessary

to renew a property *warrant* in order to complete the retrieval. *Applications* to the *Secretary of State* for renewal should state why it is being or has been closed down, why it has not been possible to remove the equipment and any timescales for removal, where known.

8. Keeping of records

Centrally retrievable records of authorisations

Directed and intrusive surveillance authorisations

8.1. A record of the following information pertaining to all *authorisations* shall be **centrally retrievable** within each *public authority* for a period of at least **three years** from the ending of each *authorisation*. This information should be regularly updated whenever an *authorisation* is granted, renewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners upon request.

- the type of *authorisation*;
- the date the *authorisation* was given;
- name and rank/grade of the *authorising officer*;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- if the *authorisation* has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the *authorising officer;*
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice[59];
- whether the *authorisation* was granted by an individual directly involved in the investigation;[60]
- the date the *authorisation* was cancelled.

8.2. The following documentation should also be centrally retrievable for at least three years from the ending of each *authorisation*:

- a copy of the *application* and a copy of the *authorisation* together with any supplementary documentation and notification of the approval given by the *authorising officer*;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the *authorising officer*;
- a record of the result of each review of the *authorisation*;
- a copy of any renewal of an *authorisation*, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction to cease surveillance was given;
- the date and time when any other instruction was given by the *authorising officer*.

Property interference authorisations

8.3. The following information relating to all *authorisations* for **property interference** should be centrally

59 See Chapter 4
60 See paragraph 5.7

retrievable for at least three years:

- the time and date when an *authorisation* is given;
- whether an *authorisation* is in written or oral form;
- the time and date when it was notified to a Surveillance Commissioner;
- the time and date when the Surveillance Commissioner notified his approval (where appropriate);
- every occasion when entry on or interference with property or with wireless telegraphy has occurred;
- the result of periodic reviews of the *authorisation*;
- the date of every renewal; and
- the time and date when any instruction was given by the *authorising officer* to cease the interference with property or with wireless telegraphy.

9. Handling of material and use of material as evidence

Use of material as evidence

9.1. Material obtained through **directed or intrusive surveillance,** or **entry on, or interference with, property or wireless telegraphy**, may be used as evidence in criminal proceedings. The admissibility of evidence is governed by the common law, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984[61] and the Human Rights Act 1998. Whilst this code does not affect the application of those rules, obtaining proper *authorisations* should help ensure the admissibility of such evidence under the common law.

9.2. Any decisions by a Surveillance Commissioner in respect of granting prior approval for intrusive surveillance activity or entry on, or interference with, property or with wireless telegraphy, (see paragraph 6.11 and 7.23) shall not be subject to appeal or be liable to be questioned in any court.[62]

Retention and destruction of material

9.3. Each *public authority* must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance or property interference. *Authorising officers* through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

9.4. Where the product of surveillance or interference with property or wireless telegraphy could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements[63] for a suitable further period, commensurate to any subsequent review.

9.5. There is nothing in the 2000 Act, 1994 Act or 1997 Act which prevents material obtained under directed or intrusive surveillance or property interference *authorisations* from being used to further other investigations.

Law enforcement agencies

9.6. In the cases of the law enforcement agencies, particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

The intelligence services, MOD and HM Forces

9.7. The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the 1989 Act and the 1994 Act.

9.8. With regard to the service police forces (the Royal Navy Police, the Royal Military Police and the Royal Air Force Police), particular attention is drawn to the Criminal Procedure and Investigations Act 1996 (Code of Practice) (Armed Forces) Order 2008, which requires that the investigator retain all material obtained in a service investigation which may be relevant to the investigation.

61 and section 76 of the Police & Criminal Evidence (Northern Ireland) Order 1989

62 see section 91(10) of the 1997 Act

63 For example, under the Criminal Procedure and Investigations Act 1996 or the Security Service Act 1989.

Use of intercepted material in applications

9.9. Material that is obtained directly as a consequence of the execution of an interception *warrant* is intercept product. Any copy, extract or summary of the material which identifies itself as intercept product, must be treated in accordance with the restrictions on the use of intercepted material.

9.10. Any copy, extract or summary of the material which identifies itself as intercept product may be used as a basis for the acquisition of other information for intelligence purposes only[64], if there is sufficient intercept product or non-intercept material available to the *authorising officer* to allow that person to consider the necessity and proportionality of acquiring the other information. The *application* to the *authorising officer* should be treated as product of the interception.

9.11. Any copy, extract or summary of the material which identifies itself as intercept product may be used as a basis for the acquisition of other information for use in legal proceedings provided that the other information does not identify itself as intercept product and there is sufficient non-intercept material available to the *authorising officer* to allow that person to consider the necessity and proportionality of acquiring the other information.

64 Section 81(5) of the 2000 Act qualifies the reference to preventing or detecting serious crime in section 5(3) – grounds for the issue of an interception warrant – to exclude gathering of evidence for use in any legal proceedings.

10. Oversight by Commissioners

10.1. The 1997 and 2000 Acts require the Chief Surveillance Commissioner to keep under review (with the assistance of the Surveillance Commissioners and Assistant Surveillance Commissioners) the performance of functions under Part III of the 1997 Act and Part II of the 2000 Act by the police (including the service police forces, the Ministry of Defence Police and the British Transport Police), SOCA, SCDEA, HMRC and the other public authorities listed in Schedule 1 of the 2000 Act [*include also reference to any Consolidating Orders*] and in Northern Ireland officials of the Ministry of Defence and HM Forces.

10.2. The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within Part II of the 2000 Act and the 1994 Act by the Security Service, Secret Intelligence Service, GCHQ and the Ministry of Defence and HM Forces (excluding the service police forces, and in Northern Ireland officials of the Ministry of Defence and HM Forces).

10.3. This code does not cover the exercise of any of the Commissioners' functions. It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

10.4. References in this code to the performance of review functions by the Chief Surveillance Commissioner and other Commissioners apply also to Inspectors and other *members* of staff to whom such functions have been delegated.

11. Complaints

11.1. The 2000 Act establishes an independent Tribunal. This Tribunal is made up of senior *members* of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction. This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal

PO Box 33220

London

SW1H 9ZQ

020 7035 3711.

12. Glossary

Application
A request made to an authorising officer to consider granting (or renewing) an authorisation for directed or intrusive surveillance (under the 2000 Act), or interference with property or wireless telegraphy (under the 1994 or 1997 Act). An application will be made by a member of a relevant public authority.

Authorisation
An application which has received the approval of an authorising officer. Depending on the circumstances, an authorisation may comprise a written application that has been signed by the authorising officer, or an oral application that has been verbally approved by the authorising officer.

Authorising officer
A person within a public authority who is entitled to grant authorisations under the 2000 or 1997 Acts or to apply to the Secretary of State for such warrants. Should be taken to include senior authorising officers.

Confidential information
Confidential personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between Members of Parliament and their constituents, or matters subject to legal privilege. See Chapter 4 for a full explanation.

Legal privilege
Matters subject to legal privilege are defined in section 98 of the 1997 Act. This includes certain communications between professional legal advisers and their clients or persons representing the client.

Private information
Any information relating to a person over which that person has a reasonable expectation of privacy. This includes information relating to a person's private, family or professional affairs. Private information includes information about any person, not just the subject(s) of an investigation.

Public authority
Any public organisation, agency or police force (including the military police forces).

Member
An employee of an organisation, or a person seconded to that organisation (for example, under the terms of section 24 of the Police Act 1996).

Officer
An officer within a public authority, or a person seconded to one of these agencies as an officer..

Secretary of State
Any Secretary of State (in practice this will generally be the Home Secretary).

Senior authorising officer
A person within a public authority who is entitled to grant intrusive surveillance authorisations under the 2000 Act or to apply to the Secretary of State for such warrants. See also Authorising officer.

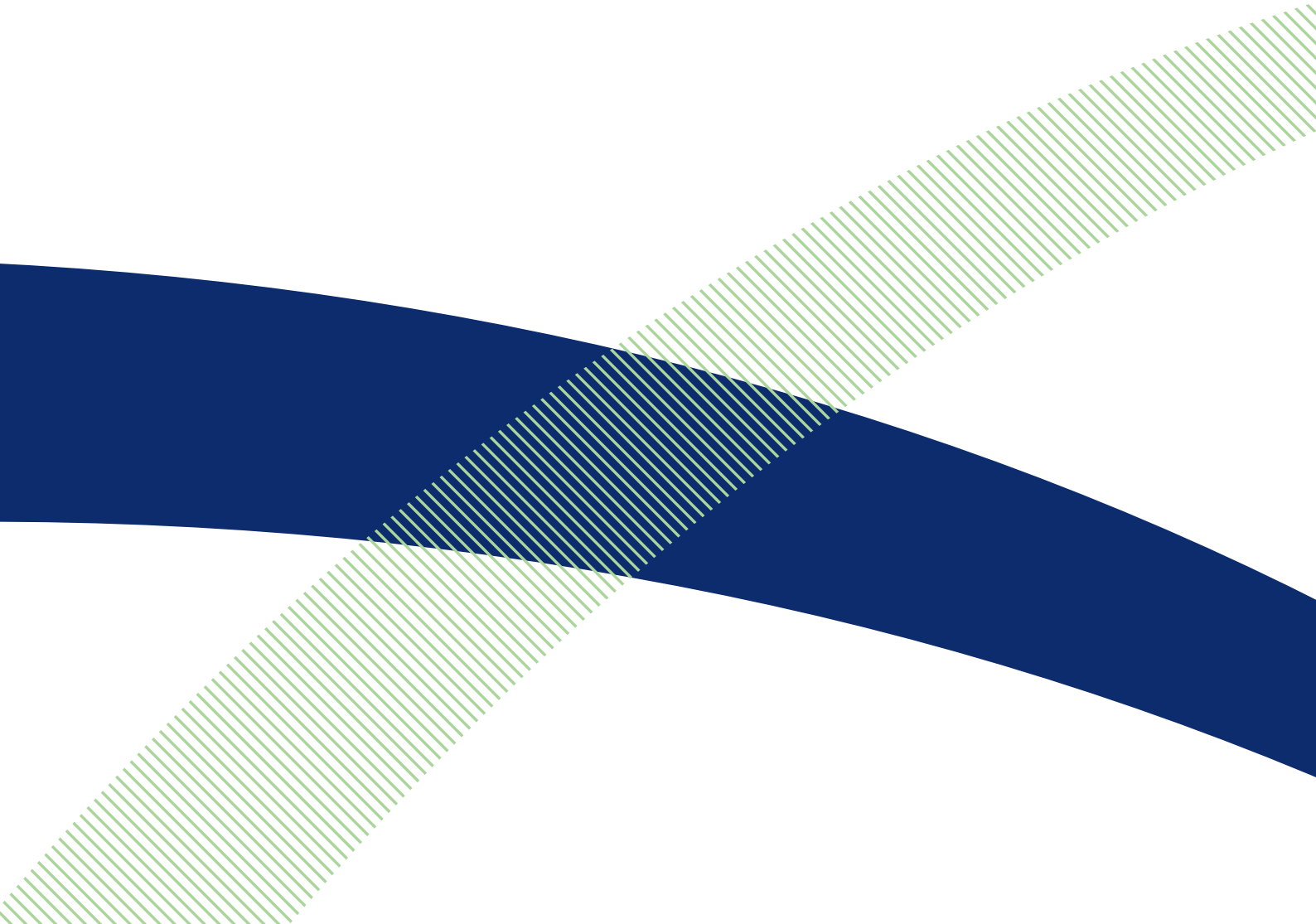
Services police
The Royal Naval Police, Royal Military Police or Royal Air Force Police.

Warrant
A type of authorisation granted by a Secretary of State following an application for intrusive surveillance or property interference under the 1994, 1997 or 2000 Acts.

Home Office

9. Draft Code of Practice on Covert Human Intelligence Sources

Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000



1. Introduction

Definitions

1.1. In this code:

- "1989 Act" means the Security Service Act 1989;
- "1994 Act" means the Intelligence Services Act 1994;
- "1997 Act" means the Police Act 1997;
- "2000 Act" means the Regulation of Investigatory Powers Act 2000;
- "RIP(S)A" means the Regulation of Investigatory Powers (Scotland) Act 2000.

Background

1.2. This code of practice provides guidance on the authorisation of the conduct or use of covert human intelligence sources (a "CHIS") by public authorities under Part II of the 2000 Act.

1.3. This code is issued pursuant to Section 71 of the 2000 Act, which stipulates that the Secretary of State shall issue one or more **codes of practice** in relation to the powers and duties in Parts I to III of the 2000 Act, section 5 of the 1994 Act and Part III of the 1997 Act. This code replaces the previous code of practice issued in 2002.

1.4. This code should be readily available to members of any relevant public authority seeking to use the 2000 Act to authorise activity by covert human intelligence sources[1] .

Effect of code

1.5. The 2000 Act provides that all **codes of practice** relating to the 2000 Act are **admissible as evidence** in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers 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. Public authorities may also be required to justify, with regard to this code, the use or grant of authorisations in general.

1.6. Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are not provisions of the code, but are included for guidance only.

Scope of covert human intelligence source activity to which this code applies

1.7. Part II of the 2000 Act provides for the authorisation of the **conduct** or **use** of **covert human intelligence sources**. The definitions of these terms are laid out in section 26 of the 2000 Act and Chapter 2 of this code. Not all human source activity will fall within these definitions and an authorisation under the 2000 Act will not therefore always be needed. Chapter 2 provides full definitions of terms and examples of activity which may or may not fall within the scope of the 2000 Act.

1.8. This code of practice is not intended to affect existing practices and procedures surrounding criminal participation of covert human intelligence sources.

1 Being those listed in or added to Part I of schedule 1 of the 2000 Act.

Basis for lawful conduct and use of covert human intelligence sources

1.9. Public authorities are not required by the 2000 Act to seek or obtain an authorisation just because one is available (see section 80 of the 2000 Act). Nevertheless, where there is an interference by a public authority with the right to respect for **private** and **family life** guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other lawful authority, the consequences of not obtaining an authorisation under the 2000 Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

1.10. Public authorities are therefore strongly recommended to seek an authorisation wherever the conduct or use of a covert human intelligence source is likely to interfere with a person's Article 8 rights to privacy by obtaining private information from or about a person, whether or not that person is the subject of the investigation or operation.[2] Obtaining an authorisation will ensure that the action is carried out in accordance with the law and subject to stringent safeguards against abuse.

1.11. However, where the conduct or use of a covert human intelligence source is such that there will be no interference with a person's Article 8 rights, an authorisation under the 2000 Act may not be needed. Public agencies are therefore encouraged to consider carefully the requirement for seeking an authorisation.

Example: *An undercover customs officer may carry out a simple test purchase at a shop (for example, to verify the level of supply of goods liable to a certain restriction or tax). The undercover officer may fit the definition of a covert human intelligence source under the 2000 Act (see Chapter 2). However, where the conduct of the officer is such that no private information will be obtained, the activity would not engage a person's Article 8 rights. An authorisation under the 2000 Act, whilst available, would not therefore be required as the activity would not otherwise be unlawful.*

Use of material as evidence

1.12. Material obtained from a covert human intelligence source may be used as evidence in criminal proceedings[3]. The admissibility of evidence is governed by the common law, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984[4] and the Human Rights Act 1998. Whilst this code does not affect the application of those rules, obtaining proper authorisations should help ensure the admissibility of evidence.

1.13. Product obtained by a covert human intelligence source is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996, where those rules apply to the law enforcement body in question.

1.14. There are also well-established legal procedures to protect the identity of a source from disclosure in such circumstances. [*Witness anonymity issues? – see DPP interim guidance on UCs and anonymous witnesses*]

Cross-border considerations

Scotland

1.15. Where all the conduct authorised is likely to take place in **Scotland**, authorisations should be granted under **RIP(S)A 2000,** unless the authorisation is being obtained by those public authorities listed in section 46(3) of the 2000 Act and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2000; SI No. 2418.

1.16. Additionally, any authorisation granted or renewed for the purposes of **national security or the economic well-being of the United Kingdom** must be made under the **2000 Act**.

2 Private information should be taken generally to include any aspect of a person's private [life] or personal relationship with others, including family and professional or business relationships. Private information may include personal data such as name, telephone numbers and address details.

3 whether these proceedings are brought by the public authority that obtained the authorisation or by another public authority (subject to handling arrangements agreed between the authorities)

4 and section 76 of the Police & Criminal Evidence (Northern Ireland) Order 1989

1.17. This code of practice is extended to Scotland in relation to authorisations made under Part II of the 2000 Act which apply to Scotland. A separate code of practice applies in relation to authorisations made under RIP(S)A.

International

1.18. Authorisations under the 2000 Act can be given for the conduct or use of a covert human intelligence source both inside and outside the United Kingdom. However, authorisations for actions outside the United Kingdom can only validate them for the purposes of civil or criminal proceedings in or before any court or tribunal[5] in the United Kingdom. An authorisation under Part II of the 2000 Act does not take into account the requirements of any country outside the United Kingdom in which the investigation or operation is taking place.[6]

1.19. Public authorities must have in place internal systems to manage any overseas source deployments. Such deployments are often only intended to impact locally and are therefore authorised under domestic law. However, public authorities should take care to monitor such deployments to identify where civil or criminal proceedings may become a prospect in the UK and ensure that, where appropriate, an authorisation under Part II of the 2000 Act is sought if this becomes the case.

1.20. The Human Rights Act 1998 applies to all activity taking place within the UK. This should be taken to include overseas territories and facilities which are within the jurisdiction of the UK. Authorisations under the 2000 Act may be therefore required for overseas operations occurring in UK Embassies, military bases, detention facilities, etc., in order to comply with rights to privacy under Article 8 of the ECHR.[7]

1.21. Members of foreign law enforcement or other agencies or covert human intelligence sources of those agencies may be authorised under the 2000 Act in the UK in support of domestic and international investigations.

5 or proceedings before an officer in respect of a service offence within the meaning of the Armed Forces Act 2006

6 Public authorities are strongly advised to seek authorisations where available under the 2000 Act for any overseas operations where the subject of investigation is a UK national or is likely to become the subject of criminal proceedings in the UK, or where the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court

7 See R v Al Skeini June 2007. If conduct is to take place overseas the ACPO Covert Investigation (Legislation and Guidance) Steering Group may be able to offer additional advice.

2. Covert human intelligence sources: definitions and examples

Definition of a covert human intelligence source (CHIS)

2.1. Under the 2000 Act, a person is a covert human intelligence source if:

a) he establishes or maintains a **personal or other relationship** with a person for the **covert purpose** of facilitating the doing of anything falling within paragraph b) or c);

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

c) he **covertly discloses information obtained** by the use of such a relationship or as a consequence of the existence of such a relationship.[8]

2.2. A relationship is established or maintained for a **covert purpose** if and only if this is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.[9]

2.3. A **relationship is used covertly**, and **information obtained is disclosed covertly**, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.[10]

Definition of conduct or use of a CHIS

2.4. Subject to the procedures outlined in Chapter 3 of this Code, an authorisation may be obtained under Part II of the 2000 Act for the **conduct** or **use** of covert human intelligence sources.

2.5. The **conduct of a CHIS** is any conduct which falls within paragraph 2.1 above or is incidental to anything falling within that paragraph.[11]

2.6. The **use of a CHIS** involves inducing, asking or assisting a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.[12]

2.7. Whether it is the **conduct** or **use** of a CHIS that requires authorisation will generally depend on whether the CHIS is a member of the general public or a member of the public agency involved in the investigation or operation:

- The activities of an undercover officer in engaging with individuals[13] as part of a covert investigation or operation will generally be authorised as the **conduct** of a CHIS.
- The activities of a member of the public performing the role of a CHIS at the request of a public authority will generally be authorised as the **use** of a CHIS;
- In rare situations where a member of the public is performing the role of a CHIS without being induced, asked or assisted by a public authority, the activities would generally be authorised as the **conduct** of a CHIS (see 2.14 below).

8 See section 26(8) of the 2000 Act
9 See section 26(9)(b) of the 2000 Act for full definition
10 See section 26(9)(c) of the 2000 Act for full definition
11 See section 26(7)(a) of the 2000 Act
12 See section 26(7)(b) of the 2000 Act
13 whether in person or remotely

Example of conduct of a CHIS *A group of individuals is suspected of operating a criminal drugs importation network. An undercover officer is inserted into the network in order to form a relationship with the individuals involved and obtain information on the nature of the operation. This activity would fall properly within the definition of conduct of a CHIS as a relationship has been established for the covert purpose of using that relationship covertly to obtain information. The activities of the undercover officer should be authorised under the 2000 Act, especially as it is likely that his activities will otherwise cause unlawful interference with privacy by virtue of the Human Rights Act 1998.*

Example of use of a CHIS *A group of individuals is suspected by the police of involvement in a crime. One of the individuals (Mr X) is approached by a police officer and is asked to obtain and provide certain information on the activities of the others. Whether or not payment is offered or made, this request constitutes use of a CHIS. Mr X is being asked to maintain his relationship with the group for the covert purpose of disclosing covertly information obtained as a consequence of that relationship. The use of Mr X as a CHIS should be authorised under the 2000 Act, especially as his subsequent activities may otherwise cause unlawful interference with privacy.*

Human source activity falling outside CHIS definition

2.8. Not all human source activity will meet the definition of a covert human intelligence source. Examples might include where a source is a public volunteer, is disclosing information out of professional or statutory duty, or has been tasked to obtain information other than by way of a relationship.

Public volunteers

2.9. In many cases involving human sources volunteering information, **no relationship** will have been established or maintained for a **covert purpose**, meaning that the source is not a covert human intelligence source and no authorisation under the 2000 Act is required.[14]

Example: *A member of the public volunteers a piece of information to the police regarding something he has witnessed in his neighbourhood. The member of the public would not be regarded as a covert human intelligence source. He is passing the information out of civic duty and not as a result of a relationship which has been established or maintained for a covert purpose.*

Example: *A caller to a confidential hotline (such as Crimestoppers, the Customs Hotline, the Anti-Terrorist Hotline, or the Security Service Public Telephone Number) reveals that he knows of criminal or terrorist activity. Even if the caller is involved in the activities on which he is reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain his relationship with those involved in order to continue to supply information, an authorisation for the use of a CHIS is likely to be appropriate.*

Professional or statutory duty

2.10. Certain individuals will be required to volunteer information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by the money laundering provisions of the Proceeds of Crime Act 2002 will be required to comply with the Money Laundering Regulations 2003 and report suspicious transactions. Similarly, financial officials, accountants or company administrators may have a duty to volunteer to the Serious Fraud Office information that they have obtained by virtue of their position.

2.11. Any such regulatory or professional disclosures should not result in these individuals meeting the definition of a CHIS, as the business or professional relationships from which the information derives will not have been established or maintained for the covert purpose of disclosing such information.

14 See Chapter 2 of this code for further guidance on types of source activity to which authorisations under Part II of the 2000 Act may or may not apply.

Tasking not involving relationships

2.12. The tasking or paying of a person to obtain information covertly will often result in the person becoming a CHIS and an authorisation under Part II of the 2000 Act will be appropriate. However, this will not be true in all circumstances. For example, where the tasking given to a person does not require that person to establish or maintain a personal or other relationship for the purpose of obtaining the information sought, that person will not be a CHIS.

Example: *An employee of a factory may be tasked by a public agency with providing factual information about the layout of the premises and its working practices for the purposes of protecting public health. The employee agrees to share this information. Where the employee does not need to establish or maintain a personal or other relationship for the purpose of providing the information, for example if he has ready access to the information as a function of his work, the employee does not become a CHIS. This holds true even if the employee is paid for the information.*

Identifying when a human source becomes a CHIS

2.13. Particular attention should be paid to the status of a human source who is not initially deemed a CHIS but who continues to provide information to a public authority. It will be important for that authority to monitor the status of the source and apply for an authorisation if that source becomes a covert human intelligence source under the definition of the 2000 Act and if there would otherwise be unlawful interference with privacy. Such a transition will often occur if the source is **tasked** or **paid** to use a relationship to find out private information.

Example: *Mr Y volunteers information to the police about a work colleague out of civic duty. Mr Y is asked by the police to provide an update if any more such information comes to his attention and agrees to do so. Mr Y is unlikely to be a CHIS at this stage as he is not maintaining (or being asked to maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information – he merely intends to disclose information if it comes to light. However, Mr Y is subsequently contacted by the police and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with colleague is being maintained and exploited for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise the interference with the colleague's privacy.*

2.14. However, the tasking or paying of a person should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so by a public authority. It is possible therefore that a person will become engaged in the **conduct of a CHIS** without a public authority inducing, asking or assisting that person.

Example: *Mr Z volunteers information to the police about a neighbour's possible criminal activities out of civic duty. As above, Mr Z is asked by the police to provide an update if any more such information comes to his attention and agrees to do so. Mr Z would not be considered a CHIS at this stage as he is not maintaining or being asked to maintain a relationship with his neighbour for the covert purpose of obtaining and disclosing information. However, Mr Z subsequently repeatedly contacts the police and provides further specific information of interest to the police about his neighbour's activities. If it becomes suspected that Mr Z is maintaining his relationship with his neighbour for the covert purpose of providing the information (even though the police have not asked him to do so), a CHIS authorisation may be appropriate to authorise the interference with the neighbour's privacy.*

3. General rules on authorisations

Overview

3.1. An authorisation under Part II of the 2000 Act for the conduct or use of a CHIS will provide lawful authority for any such activity involving the conduct or use of a CHIS as is specified or described in the authorisation, is carried out by or in relation to the person to whose actions as a CHIS the authorisation relates and is carried out for the purposes of, or in connection with, the investigation or operation so described.[15]

3.2. Responsibility for giving the authorisation will depend on which public authority is responsible for the CHIS. For the purposes of this and future chapters, the person in a public authority responsible for granting an authorisation will be referred to as the "authorising officer". The relevant authorities and authorising officers are listed in [Consolidating order].

3.3. Where possible, the **same authorising officer** as grants an authorisation should be responsible for considering subsequent reviews and renewals of that authorisation and any related security and welfare issues (see paragraphs 6.11-6.13).

Necessity and Proportionality

3.4. The 2000 Act stipulates that the authorising officer must believe that an authorisation for the conduct or use of a CHIS is **necessary** in the circumstances of the particular case for one or more of the statutory grounds listed in section 29(3) of the 2000 Act.

3.5. If the conduct or use of the CHIS is deemed necessary, the authorising officer must also believe that the conduct or use is **proportionate** to what is sought to be achieved by carrying it out. This involves balancing the likely intrusion into the privacy of the target of the investigation (or any other person who may be affected) against the expected benefit to the investigation.

3.6. When assessing proportionality, authorising officers should consider both the nature of the offence being investigated and the benefits that the use of a CHIS will bring to the investigation. The fact that a suspected offence is serious will not alone render the use of a CHIS proportionate. Similarly, some offences may be so minor that the use of a CHIS would not be proportionate. It is quite possible that an intrusive action that is judged highly likely to produce information of significant benefit to an investigation into a relatively minor crime may be more justifiable than a similarly intrusive action which cannot be expected to produce any useful or new intelligence in a serious crime investigation.

3.7. Any CHIS activity should have a proportionate expected or potential benefit for the investigation and should not be excessive or arbitrary. No activity should be considered proportionate if the information which is sought could be **reasonably obtained by other less intrusive means** without detriment to the investigation.

3.8. In the above context, it is important that those involved in the use or conduct of a CHIS are fully aware of the extent and limits of the authorisation in question.

Collateral Intrusion

3.9. Before authorising the conduct or use of a source, the authorising officer should also take into account the risk of intrusion into the privacy of persons who are not the intended targets of the CHIS activity (collateral intrusion).

15 See section 29(4) of the 2000 Act.

3.10. Measures should be taken, wherever practicable, to avoid or minimize unnecessary intrusion into the private lives of those who are not the intended targets of the CHIS activity. Where such collateral intrusion is unavoidable, the activities may still be authorised providing this collateral intrusion is considered proportionate to the aims of the intended intrusion.

3.11. All applications should therefore include an assessment of the risk of any collateral intrusion and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed use and conduct of a CHIS.

3.12. Note that where CHIS activity is deliberately proposed against individuals who are not suspected of direct or culpable involvement in the matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such interference should be carefully considered against the necessity and proportionality criteria as described above (paragraphs 3.4-3.8).

Example 1: *An undercover officer is deployed to obtain information about the activities of a suspected criminal gang under a conduct of CHIS authorisation. It is assessed that the officer will in the course of this deployment obtain private information about some individuals who are not involved in criminal activities and are of no interest to the investigation. The authorising officer should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the conduct of CHIS authorisation.*

Reviewing authorisations

3.13. Where the nature or extent of collateral intrusion becomes greater than that anticipated in the original authorisation, the authorising officer should reconsider the proportionality of the operation at a review and this should be highlighted at the next renewal.

3.14. Where a CHIS authorisation provides for interference with the privacy of initially unidentified individuals whose identity is later established, the terms of the authorisation should be refined at a review to include the identity of these individuals. This process will not require a fresh authorisation, providing the scope of the original authorisation envisaged interference with the privacy of such individuals.

Example: *An authorisation is obtained by the police to authorise a CHIS to use her relationship with "Mr X and his associates" for the covert purpose of providing information relating to their suspected involvement in a crime. Mr X introduces the CHIS to Mr A. It is assessed that obtaining more information on Mr A will assist the investigation. The CHIS may use her relationship with Mr A to obtain such information (he is an associate of X) but the authorisation should be amended by means of a review to specify interference with the privacy of "Mr X and his associates, including Mr A."*

3.15. Any proposed changes to the nature of the CHIS operation (i.e. the activities involved) should be brought to the attention of the authorising officer at a review. The authorising officer should consider whether the proposed changes are proportionate (bearing in mind any extra intrusion into privacy or collateral intrusion), before approving or rejecting them. Any such changes should be highlighted at the next renewal. (See Chapter 6 on Management of Covert Human Intelligence Sources.)

Participation in criminal activity

3.16. In a very limited range of circumstances an authorisation under Part II may, by virtue of sections 26(7) and 27 of the 2000 Act, render lawful conduct which would otherwise be criminal, if it is conduct falling within section 26(8) of the 2000 Act which the source is authorised to undertake or is incidental to any such conduct. This would depend on the circumstances of each individual case, and consideration should always be given to seeking advice from the legal adviser within the relevant public authority when such activity is contemplated. A source that acts beyond the limits recognised by the law will be at risk from prosecution. The need to protect the source cannot alter this principle.

Local considerations and risk assessments

3.17. Any person granting or applying for an authorisation will also need to be aware of any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the conduct or use of a CHIS or use of information obtained from that CHIS.

3.18. It is therefore recommended that where an authorising officer from a public authority considers that conflicts might arise they should consult a senior officer within the police force area in which the CHIS is deployed.

3.19. The authorising officer should also make an assessment of any personal risk to a CHIS in carrying out the conduct in the proposed authorisation.

Combined authorisations

3.20. A single authorisation may combine two or more different authorisations under Part II of the 2000 Act [16]. For example, a single authorisation may combine authorisations for intrusive surveillance and the conduct of a CHIS. In such cases the provisions applicable to each of the authorisations must be considered separately by the appropriate authorising officer. Thus, a police superintendent can authorise the conduct of a CHIS but an authorisation for intrusive surveillance by the police needs the separate authority of a chief constable (and, in certain cases, the approval of a Surveillance Commissioner).

3.21. Where an authorisation for the use or conduct of a covert human intelligence source is combined with a Secretary of State authorisation for intrusive surveillance, the combined authorisation must be issued by the Secretary of State.

3.22. The above considerations do not preclude public authorities from obtaining separate authorisations.

Operations involving multiple undercover officers

3.23. A single authorisation under Part II of the 2000 Act may be used to authorise the conduct of more than one CHIS. However, this is only likely to be appropriate for operations involving the conduct of several undercover officers acting as CHISs in situations where the activities to be authorised, the targets of the operation, the interference with privacy, the likely collateral intrusion and the risk assessments are the same for each officer.

3.24. In such situations, a conduct of CHIS authorisation for undercover officer activity will provide a lawful basis for the interference with the privacy of certain individuals in a certain way, regardless of which undercover officer conducts that activity. The undercover officers need not necessarily be individually identified at the time of the authorisation and need not be the subject of separate CHIS authorisations. However, the application for the conduct of a CHIS authorisation should make clear the intended scope of the operation in order for the authorising officer to consider the necessity and proportionality of the proposal.

16 See section 43(2) of the 2000 Act.

Example: *A police undercover operation is planned to obtain information about a suspected tax avoidance racket. It is anticipated that a small number of undercover officers will need to be deployed to obtain information on the individuals suspected of wrongdoing. A single CHIS authorisation may be sought, stating the approximate number of undercover officers to be deployed and indicating clearly the activities which they are to undertake. Should a further undercover officer later need to be introduced to the operation to conduct the same activities, or to replace an existing officer, the interference with privacy arising from this will be authorised under the original authorisation. It may however be appropriate to convene a review with the authorising officer to confirm that there are no specific further risks associated with the deployment of the officer in question and that the officer does not require any further activities to be authorised (see Reviewing Authorisations above).*

3.25. Note that although a single authorisation can authorise the conduct of multiple undercover officers, a **separate record** of the activities of each officer acting as a CHIS is required to be maintained in accordance with section 29(5) of the 2000 Act and the Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 272 (see Chapter 5).

Directed surveillance of a potential CHIS

3.26. It may be necessary to deploy directed surveillance against a potential CHIS as part of the process of assessing their suitability for recruitment, or in planning how best to make the approach to them. An authorisation under this code authorising an officer to establish a covert relationship with a potential CHIS could be combined with a directed surveillance authorisation so that both the officer and potential source could be followed. Directed surveillance is defined in section 26(2) of the 2000 Act. See the code of practice on Covert Surveillance and Property Interference.

Additional rules

Recording of telephone conversations

3.27. Subject to paragraph 3.28 below, the interception of communications sent by post or by means of public telecommunications systems or private telecommunications systems attached to the public network may be authorised only by the Secretary of State, in accordance with the terms of Part I of the 2000 Act. Nothing in this code should be taken as granting dispensation from the requirements of that Part of the 2000 Act.

3.28. Part I of the 2000 Act provides certain exceptions to the rule that interception of telephone conversations must be warranted under that Part. This includes, where one party to the communication consents to the interception, it may be authorised in accordance with section 48(4) of the 2000 Act provided that there is no interception warrant authorising the interception. In such cases, the interception is treated as directed surveillance (see chapter 2 of the Covert Surveillance and Property Interference).

Use of covert human intelligence source with technical equipment

3.29. A CHIS wearing or carrying a surveillance device does not need a separate intrusive or directed surveillance authorisation to authorise the use of that device provided it will only be used in the presence of the CHIS. However, if a surveillance device is to be used other than in the presence of the CHIS, an intrusive or directed surveillance authorisation and, if applicable, an authorisation for interference with property should be obtained. See the Directed and Intrusive Surveillance Code of Practice.

3.30. A CHIS, whether or not wearing or carrying a surveillance device, who is invited into residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or vehicle which take place in his presence. This also applies to the recording of telephone conversations other than by interception which takes place in the source's presence. Authorisation for the conduct or use of that source may be obtained in the usual way.

4. Confidential, legally privileged or Parliamentary material

Overview

4.1. The 2000 Act does not provide any special protection for 'confidential information'. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to **legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material**. So, for example, extra care should be taken where, through the conduct or use of a CHIS, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or between an Member of Parliament and a constituent relating to private constituency matters, or wherever matters of medical or journalistic confidentiality or legal privilege may be involved.

4.2. References to a Member of Parliament include references to a Member of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

4.3. In cases where through the conduct or use of a CHIS it is likely that knowledge of confidential information will be acquired, the deployment of the CHIS is subject to a higher level of authorisation. Annex A lists the authorising officer for each public authority permitted to authorise such conduct or use of a CHIS.

[The following passage relating to legal professional privilege reflects the content of a statutory instrument under s. 29 RIPA which the Home Secretary intends to bring before Parliament, subject to the outcome of this consultation.]

4.4. Subject to paragraph 4.5 below, the conduct or use of a CHIS to obtain, provide access to or disclose legally privileged material shall not be undertaken without the prior approval of a Surveillance Commissioner (with the exception of *authorisation*s requiring the approval of the *Secretary of State*). Such *authorisation*s shall only be approved if the Commissioner is satisfied that there are reasonable grounds for believing that:

a) the authorisation is necessary in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom; and

b) the authorised conduct or use is proportionate to what is sought to be achieved by that conduct or use.

4.5. With the exception of urgent *applications*, the *authorisation* shall not take effect until such time as:

a) the *authorisation* has been approved by a Surveillance Commissioner; and

b) written notice of the Commissioner's decision to approve the *authorisation* has been given to the *authorising officer*.]

Communications subject to Legal Privilege

4.6. Section 98 of the 1997 Act describes those matters that are subject to legal privilege in England and Wales. In Scotland, the relevant description is contained in section 33 of the Criminal Law (Consolidation) (Scotland) Act 1995. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.

4.7. Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if there are grounds to believe, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose. But 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 applies to the provision of professional legal advice by any individual, agency or organisation qualified to provide it.

4.8. The 2000 Act does not provide any special protection for legally privileged information. Nevertheless, such information is particularly sensitive and surveillance which acquires such material may engage Article 6 of the ECHR (right to a fair trial) as well as Article 8. Legally privileged information obtained by a CHIS is extremely unlikely ever to be admissible as evidence in criminal proceedings. Moreover, the mere fact that use has been made of a CHIS to obtain such information may lead to any related criminal proceedings being stayed as an abuse of process. Accordingly, action which may lead to such information being acquired is subject to additional safeguards under this code.

4.9. In general, an application for the conduct of use of a CHIS which is likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances. Full regard should be had to the particular proportionality issues such conduct or use of a CHIS raises. The application should include, in addition to the reasons why the conduct or use of a CHIS is considered necessary, an assessment of how likely it is that information subject to legal privilege will be acquired. In addition, the application should clearly state whether the purpose (or one of the purposes) of the conduct of use of a CHIS is to obtain legally privileged information.

4.10. This assessment will be taken into account by the authorising officer in deciding whether the proposed conduct or use of a CHIS is necessary and proportionate for a purpose under section 29 of the 2000 Act. The authorising officer may require regular reporting so as to be able to decide whether the authorisation should continue. In those cases where legally privileged information has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested.

4.11. A substantial proportion of the communications between a lawyer and his client(s) may be subject to legal privilege. Therefore, any case where a lawyer is the subject of an investigation or operation should be notified to the relevant Commissioner or Inspector during his next inspection and any material which has been retained should be made available to him if requested.

4.12. Where there is any doubt as to the handling and dissemination of information which may be subject to legal privilege, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the material takes place. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception. The retention of legally privileged information, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information. Any dissemination of legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

Communications involving Confidential Information

4.13. Similar consideration must also be given to authorisations that involve **confidential personal information, confidential constituent information** and **confidential journalistic material**. Where such material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested.

4.14. **Confidential personal information** is information held in confidence relating to the **physical or mental health** or **spiritual counselling** of a person (whether living or dead) who can be identified from it. [17]

17 **Spiritual counselling** means conversations between a person and a religious authority acting in an official capacity, where the individual being counselled is seeking or the religious authority is imparting forgiveness, absolution or the resolution of conscience in accordance with their faith.

Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

4.15. **Confidential constituent information** is information relating to communications between a Member of Parliament and a constituent in respect of constituency matters. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

4.16. **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.

4.17. [Where there is any doubt as to the handling and dissemination of **confidential information**, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the material takes place. Any dissemination of confidential material to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.]

Vulnerable individuals

4.18. A **vulnerable individual** is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a CHIS in the most exceptional circumstances. In these cases, [Annex A / consolidating order] lists the authorising officer for each public authority permitted to authorise the use of a vulnerable individual as a CHIS.*

Juvenile sources

4.19. Special safeguards also apply to the conduct or use of juveniles sources; that is sources under the age of 18 years. **On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him**. In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. Authorisations for juvenile sources should be granted by those listed in the attached table at Annex A. The duration of such an authorisation is **one month from the time of grant or renewal** (instead of twelve months). For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

* (Details listed in chapter 7 of this consultation paper.

5. Authorisation procedures for covert human intelligence sources

Authorisation criteria

5.1. Under section 29(3) of the 2000 Act an authorisation for the conduct or use of a CHIS may be granted by the authorising officer where he believes that the authorisation is necessary:

- in the interests of national security[18,19] ;
- for the purpose of preventing and detecting [20] crime or of preventing disorder;
- in the interests of the economic well-being of the UK;
- in the interests of public safety;
- for the purpose of protecting public health[21];
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
- for any other purpose prescribed in an order made by the Secretary of State [22].

5.2. The authorising officer must also believe that the authorised conduct or use of CHIS is proportionate to what is sought to be achieved by that conduct or use.

Relevant public authorities

5.3. The public authorities entitled to authorise the conduct or use of a CHIS are those listed in Schedule 1 to the 2000 Act. The specific purposes for which each public authority may obtain an authorisation for the conduct or use of a CHIS are laid out in [Consolidated Order].

Authorisation procedures

5.4. Responsibility for authorising the conduct or use of a CHIS rests with the authorising officer and all authorisations require the personal authority of the authorising officer. The Regulation of Investigatory Powers (Prescriptions of Offices, Ranks and Positions) Order 2000; SI No: 2417 [*adjust for consolidating order*] designates the authorising officer for each different public authority and the officers entitled to act only in urgent cases. In certain circumstances the Secretary of State will be the authorising officer (see section 30(2) of the 2000 Act).

5.5. The authorising officer must give authorisations in writing, except that in urgent cases, they may be given orally by the authorising officer or the officer entitled to act in urgent cases. In such cases, a statement

18 One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. These functions extend throughout the United Kingdom. An authorising officer in another public authority should not issue an authorisation under Part II of the 2000 Act where the operation or investigation falls within the responsibilities of the Security Service as set out above, except where it is to be carried out by a Special Branch or where the Security Service has agreed that another public authority can authorise the conduct or use of a CHIS which would normally fall within the responsibilities of the Security Service.

19 HM Forces may also undertake operations in connection with a military threat to national security and other operations in connection with national security in support of the Security Service, the Police Service of Northern Ireland or other Civil Powers.

20 Detecting crime is defined in section 81(5) of the 2000 Act. Preventing and detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

21 This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

22 This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

that the authorising officer has expressly authorised the action should be recorded in writing by the applicant as a priority. This should be done by the person with whom the authorising officer spoke. This statement need not contain the full detail of the application, which should however subsequently be recorded in writing when reasonably practical (generally the next working day).

5.6. 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 operation or investigation 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.

5.7. Authorising officers should not be responsible for authorising their own activities, e.g. those in which they, themselves, are to act as the CHIS or in tasking the CHIS. However, it is recognised that this is not always possible, especially in the cases of small organisations, or where it is necessary to act urgently or for security reasons. Where an authorising officer authorises his own activity the central record of authorisations (see Chapter 7) should highlight this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

[The following provisions are subject to changes contained in the Policing and Crime Bill currently before Parliament:

5.8. Subject to paragraph 5.9, authorising officers within the Police, SCDEA and SOCA may only grant authorisations on application by a member of (or person fully seconded to) their own force or agency. Authorising officers within HMRC may only grant authorisations on application by an officer of Revenues and Customs.

5.9. With regard to police forces maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London), the Metropolitan police force and the City of London police force, the restrictions outlined in paragraph 5.8 may be varied in accordance with collaboration agreements made under section 23 of the Police Act 1996. With regard to police forces maintained under section 1 of the Police (Scotland) Act 1967, the restrictions in paragraph 5.8 may be varied in accordance with collaboration agreements made under section 12 of the Police (Scotland) Act 1967.]

Information to be provided in applications for authorisation

5.10. An application for authorisation for the conduct or use of a source should be in writing and record:

- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in section 29(3) of the 2000 Act;
- the purpose for which the source will be tasked or deployed (e.g. in relation to an organised serious crime, espionage, a series of racially motivated crimes etc);
- where a specific investigation or operation is involved, nature of that investigation or operation;
- the nature of what the source will be tasked to do;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the authorisation;
- the reasons why the authorisation is considered proportionate to what it seeks to achieve;
- the level of authority required (or recommended, where that is different); and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

5.11. Additionally, in urgent cases, the authorisation should record (as the case may be):

- the reasons why the authorising officer or the officer entitled to act in urgent cases considered the case so

urgent that an oral instead of a written authorisation was given; and/or

- the reasons why it was not reasonably practicable for the application to be considered by the authorising officer.

5.12. Where the authorisation is oral, the detail referred to above should be recorded in writing by the applicant when reasonably practicable (generally the next working day).

Duration of authorisations

5.13. A written authorisation will, unless renewed, cease to have effect at the end of a period of **twelve months** beginning with the day on which it took effect.

5.14. Urgent oral authorisations or authorisations granted or renewed by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after **seventy-two hours**, beginning with the time when the authorisation was granted.

Reviews

5.15. Regular reviews of authorisations should be undertaken to assess the need for the use of a CHIS to continue. The review should include the use made of the CHIS during the period authorised, the tasks given to the CHIS and the information obtained from the CHIS. The results of a review should be retained for at least three years (see Chapter 7). Particular attention is drawn to the need to review authorisations frequently where the use of a CHIS provides access to confidential information or involves significant collateral intrusion.

5.16. In each case the authorising officer within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

Renewals

5.17. Before an authorising officer renews an authorisation, he must be satisfied that a review has been carried out of the use of a CHIS as outlined in paragraph 5.14.

5.18. If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of **twelve months**. Renewals may also be granted orally in urgent cases and last for a period of **seventy-two hours**.

5.19. A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. **An application for renewal should therefore not be made until shortly before the authorisation period is drawing to an end**.

5.20. Any person who would be entitled to grant a new authorisation can renew an authorisation. However, where possible the same authorising officer as granted the original authorisation should consider the renewal.

5.21. Authorisations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorisation. Documentation of the renewal should be retained for at least three years (see Chapter 7).

5.22. All applications for the renewal of an authorisation should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information in paragraph 5.9;
- the reasons why it is necessary to continue to use the CHIS;

- the use made of the CHIS in the period since the grant or, as the case may be, latest renewal of the authorisation;
- the tasks given to the CHIS during that period and the information obtained from the conduct or use of the CHIS; and
- the results of regular reviews of the use of the CHIS.

Cancellations

5.23. The authorising officer who granted or renewed the authorisation must cancel it if he is satisfied that the conduct or use of the CHIS no longer satisfies the criteria for authorisation or that satisfactory arrangements for the CHIS's case no longer exist. Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer (see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794) [*– adjust for Consolidating Orders*].

5.24. Where necessary, the safety and welfare of the source should continue to be taken into account after the authorisation has been cancelled.

6. Management of covert human intelligence sources

Tasking

6.1. Tasking is the assignment given to the CHIS by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the conduct or use of a CHIS is required prior to any tasking where such tasking requires the CHIS to establish or maintain a personal or other relationship for a covert purpose.

6.2. It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If this changes, then a new authorisation may need to be sought.

6.3. It is difficult to predict exactly what might occur each time a meeting with a CHIS takes place, or the CHIS meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient it should either be updated at a review (for minor amendments only) or it should cancelled and a new authorisation should be obtained before any further such action is carried out.

6.4. Similarly where it is intended to task a CHIS in a new way or significantly greater way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

Management responsibility

Handlers and controllers

6.5. Public authorities should ensure that arrangements are in place for the proper oversight and management of CHISs, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each CHIS.

6.6. The person referred to in section 29(5)(a) of the 2000 Act (the "**handler**") will have day to day responsibility for:

- dealing with the CHIS on behalf of the authority concerned;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

6.7. The handler of a CHIS will usually be of a rank or position below that of the authorising officer.

6.8. The person referred to in section 29(5)(b) of the 2000 Act (the "**controller**") will be responsible for the general oversight of the use of the CHIS.

Joint working

6.9. In cases where the authorisation is for the conduct or use of a CHIS whose activities benefit more than a single public authority, responsibilities for the management and oversight of that CHIS may be taken up by one authority or can be split between the authorities. The controller and handler of a CHIS need not be from same public authority.

6.10. It will be prudent in such situations however for the public authorities involved to lay out in writing their agreed oversight arrangements.

Security and welfare

6.11. Any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and to foreseeable consequences to others of that tasking. Before authorising the conduct or use of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset.

6.12. The CHIS **handler** is responsible for bringing to the attention of the CHIS **controller** any concerns about the personal circumstances of the CHIS, insofar as they might affect

- the validity of the risk assessment
- the conduct of the CHIS, and
- the safety and welfare of the CHIS.

6.13. Where deemed appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

7. Keeping of records

Centrally retrievable record of authorisations

7.1. A record of all CHIS authorisations covering a period of at least **three years** from the ending of each authorisation shall be **centrally retrievable** within each public authority. This record need only contain the name or codename of the CHIS, the date the authorisation was granted, renewed or cancelled and an indication as to whether the activities were self-authorised (see paragraph 5.7).

7.2. This information should be regularly updated whenever an authorisation is granted, renewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners upon request.

Individual records of authorisation and use of CHIS

7.3. Proper records must be kept of the authorisation and use made of a CHIS. Section 29(5) of the 2000 Act provides that an authorising officer must not grant an authorisation for the use or conduct of a CHIS unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records.

7.4. Public authorities are encouraged to consider maintaining such records also for human sources who do not meet the definition of a CHIS. This may assist authorities to monitor the status of a human source and identify whether that source becomes a CHIS (see paragraphs 2.13-2.14).

Further documentation

7.5. In addition, records or copies of the following, as appropriate, should be kept by the relevant authority for at least three years:

- a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the CHIS;
- the circumstances in which tasks were given to the CHIS;
- the value of the CHIS to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation;
- the date and time when any instruction was given by the authorising officer to cease using a CHIS.

7.6. The records kept by public authorities should be maintained in such a way as to preserve the confidentiality of the CHIS and the information provided by that CHIS.

8. Handling of material

Retention and destruction of material

8.1. Each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the conduct or use of a CHIS. Authorising officers must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

8.2. Where the product of the conduct or use of a CHIS could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

8.3. There is nothing in the 2000 Act which prevents material obtained from authorisations for the conduct or use of a CHIS from being used to further other investigations.

Law enforcement agencies

8.4. In the case of the law enforcement agencies, particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

The intelligence services, MOD and HM Forces

8.5. The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the 1989 Act and the 1994 Act.

8.6. With regard to the service police forces (the Royal Navy Police, the Royal Military Police and the Royal Air Force Police), particular attention is drawn to the Criminal Procedure and Investigations Act 1996 (Code of Practice) (Armed Forces) Order 2008, which requires that the investigator retain all material obtained in a service investigation which may be relevant to the investigation.

9. Oversight by Commissioners

9.1. The 2000 Act requires the Chief Surveillance Commissioner to keep under review (with the assistance of the Surveillance Commissioners and Assistant Surveillance Commissioners) the performance of functions under Part III of the 1997 Act and Part II of the 2000 Act by the police (including the service police forces, the Ministry of Defence Police and the British Transport Police), SOCA, SCDEA, HMRC and the other public authorities listed in Schedule 1 of the 2000 Act [*include also reference to any Consolidating Orders*] and in Northern Ireland officials of the Ministry of Defence and HM Forces.

9.2. The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within Part II of the 2000 Act and the 1994 Act by the Security Service, Secret Intelligence Service, GCHQ and the Ministry of Defence and HM Forces (excluding the service police forces, and in Northern Ireland officials of the Ministry of Defence and HM Forces);

9.3. This code does not cover the exercise of any of the Commissioners' functions. It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

9.4. References in this code to the performance of review functions by the Chief Surveillance Commissioner and other Commissioners apply also to Inspectors and other members of staff to whom such functions have been delegated.

10. Complaints

10.1. The 2000 Act establishes an independent Tribunal. This Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction. This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal

PO Box 33220

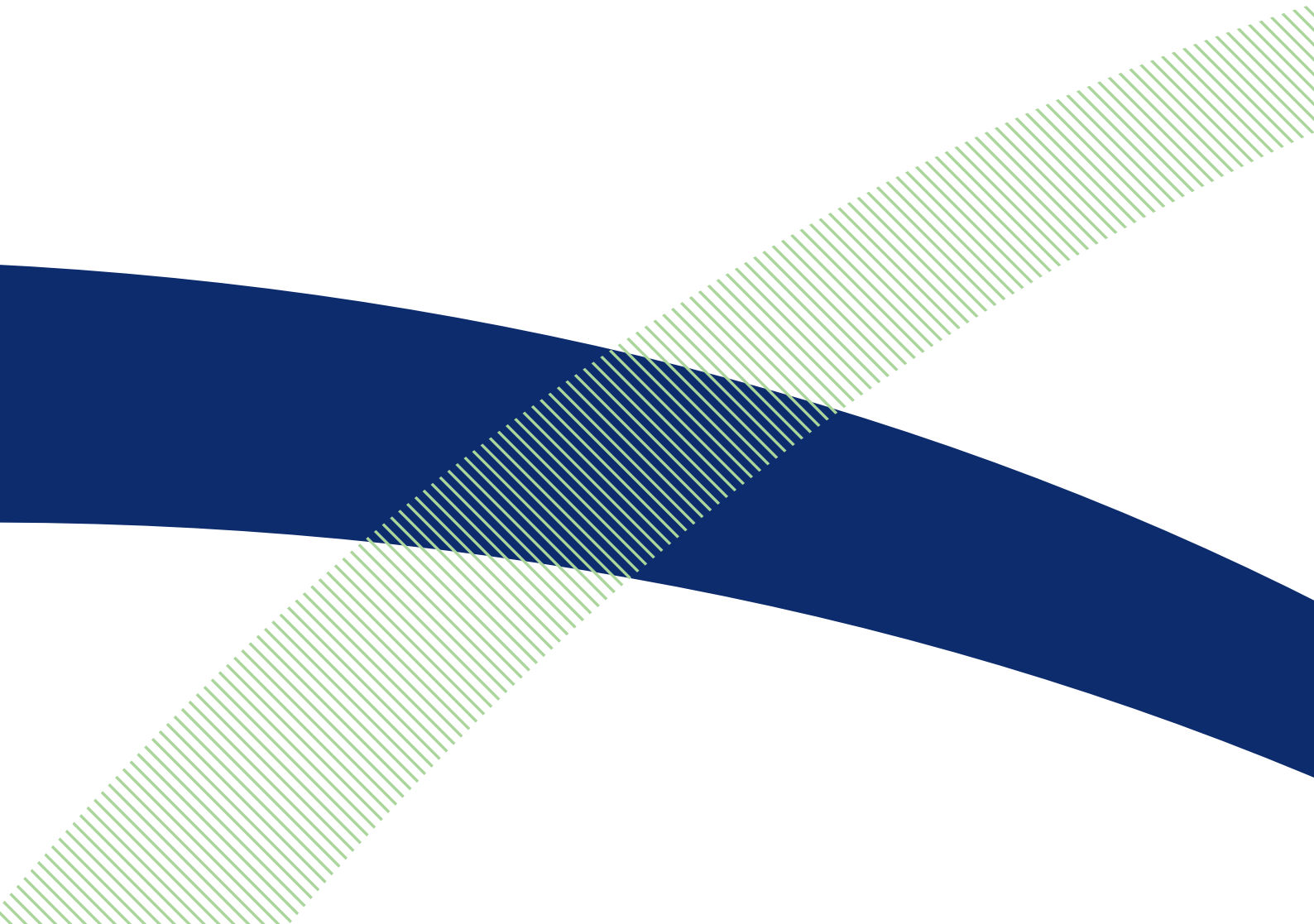
London

SW1H 9ZQ

020 7035 3711.

Home Office

Annexes



Annex A

SUMMARY

Scope of the Consultation

Topic of this consultation:	Updating the regulation of public authority use of key covert investigatory techniques. See the 'Introduction'.
Scope of this consultation:	The purpose of the present consultation is to give an opportunity to the public to comment on the Government's proposals for two Consolidating Orders and draft Codes of Practice, available on the Home Office website: http://www.homeoffice.gov.uk/.
Geographical scope:	UK-wide.
Impact Assessment	No Impact Assessment has been prepared as these proposals would simply update previous Orders laid before Parliament.

Basic Information

To:	The Government would particularly like to hear from members of the public, campaigning groups and specialist organisations concerned with the provision of public authority services and human rights considerations.
Duration:	Twelve weeks to 10 July 2009.
Enquiries:	For enquiries about the content or scope of the consultation, requests for hard copies, information about consultation events, etc: Tony Cooper, Home Office, 5th Floor Peel Building, 2 Marsham Street, London SW1P 4DF (telephone: 020 7035 1218).
How to respond:	By e-mail to commsdata@homeoffice.gsi.gov.uk; or By post to Tony Cooper, Home Office, 5th Floor Peel Building, 2 Marsham Street, London SW1P 4DF.
Additional ways to become involved:	Further background and guidance on public authority use of covert investigatory powers is available in the following publications: • Explanatory Notes to The Regulation of Investigatory Powers Act 2000; and • the existing statutory Codes of Practice on Covert Surveillance, Covert Human Intelligence Sources and Communications Data.
After the consultation:	The Government intends to publish on the Home Office website a summary of the responses received before considering what proposals to put before Parliament.

Background

Getting to this stage:	Parliament has approved six previous Orders - in 2003, 2005 and 2006 - regulating and updating public authority use of particular covert techniques. To avoid having to look across several Orders to see which public authorities are able to use covert techniques under RIPA, and in what circumstances, the Government has said that the next update will take the form of Consolidating Orders that brigade this information together into one Order for Covert Surveillance and Covert Human Intelligence Sources, and one Order for Communications Data.
Previous engagement:	The Government consulted on the original proposals for public authority use of communications data in 2003 and on the revised Code of Practice on the Acquisition and Disclosure of Communications Data in 2006. The revised Code was published in 2007.

Annex B

THE SEVEN CONSULTATION CRITERIA

The Government's new Code of Practice on Consultation, which came into effect on 1st November 2008, sets out seven best practice consultation criteria. They are:

- Criterion 1 - When to consult - Formal consultation should take place at a stage when there is scope to influence the policy outcome.
- Criterion 2 - Duration of consultation exercises - Consultations should normally last for at least 12 weeks with consideration given to longer timescales where feasible and sensible.
- Criterion 3 - Clarity of scope and impact - Consultation documents should be clear about the consultation process, what is being proposed, the scope to influence and the expected costs and benefits of the proposals.
- Criterion 4 - Accessibility of consultation exercises - Consultation exercises should be designed to be accessible to, and clearly targeted at, those people the exercise is intended to reach.
- Criterion 5 - The burden of consultation - Keeping the burden of consultation to a minimum is essential if consultations are to be effective and if consultees' buy-in to the process is to be obtained.
- Criterion 6 - Responsiveness of consultation exercises - Consultation responses should be analysed carefully and clear feedback should be provided to participants following the consultation.
- Criterion 7 - Capacity to consult - Officials running consultations should seek guidance in how to run an effective consultation exercise and share what they have learned from the experience.

The full Code of Practice is available at: http://www.berr.gov.uk/whatwedo/bre/consultation-guidance/page44420.html.

Consultation Co-ordinator

If you have any complaints or comments specifically about the consultation process, you should contact the Home Office Consultation Co-ordinator Nigel Lawrence:

- by e-mail at: nigel.lawrence@homeoffice.gsi.gov.uk; or
- by post to: Nigel Lawrence, Consultation Co-ordinator, Performance and Delivery Unit, Home Office, 3rd Floor Seacole Building, 2 Marsham Street, London SW1P 4DF

Please DO NOT send your response to this consultation to Nigel Lawrence. The Consultation Co-ordinator works to promote best practice standards set by the Government's Code of Practice, advises policy teams on how to conduct consultations and investigates complaints made against the Home Office. He does not process your response to this consultation.