Chapter 32 – Index

32. Intelligence

The Recording and Dissemination of Intelligence Material Code of Practice

In recognition of the need for European Convention on Human Rights (ECHR) compliant procedures, a working party consisting of the Association of Chief Police Officers (ACPO), Customs, the National Crime Squad (NCS) and the National Crime Intelligence Service (NCIS) has produced a voluntary Code of Practice covering **"The Recording and Dissemination of Intelligence Material".** In order to ensure Human Rights Act 1998 (HRA) compliance, IND must formalise the way in which it handles intelligence information. It has therefore agreed to abide by the Code of Practice produced by the working party.

The Code has been adapted to meet the needs of IND, but briefly, collection, handling or dissemination of intelligence information about living individuals by IND staff must be for one of the following reasons:

- in the interests of national security;
- the prevention of crime and disorder;
- The economic well-being of the country.

Additionally, to show that the processing of intelligence information about an individual, which may interfere with their (qualified) HRA rights, is legitimate, we must be able to demonstrate that:

- the information has been obtained and processed in accordance with the law (in particular, the investigatory method must not be unlawful);
- processing is necessary for the pursuance of a legitimate aim (i.e. one of the purposes specified in the preceding bullet points above);
- Processing is proportionate (commensurate with the seriousness of the offence under investigation).

A copy of the Code of Practice can be found at Annex D.

See also: IDIs Chapter 24 for further information.

32.1 Disclosure and the Freedom of Information Act

One of the main findings of the review on the enforcement of the immigration laws was that, subject to certain safeguards, there should be more sharing of information between government departments and other public bodies. The intention is to enable immigration offenders to be more readily detected and to ensure that public funds go only to those who are entitled to them.

The coming into force of the Freedom of Information Act (FOIA) has seen new processes put in place to deal with requests from the public, solicitors, agents etc for disclosure of information. It is vitally important that these processes are followed.

Under the FOI Act the right of access to all information (except that which is legally excepted) held by public authorities came into force on 1 January 2005 and affects the Data Protection Act 1998 (DPA) in two key ways;

- it extends the right of subject access to all recorded information held by IND (handled by the Subject Access Bureau (SAB));

- It provides an exemption from the duty to supply personal data under the FOIA, directing such requests back to the DPA.

Requests for information do not have to mention the legislation under which they are requesting that information.

For more detailed information, refer to IDIs chapter 24 or, for particularly difficult cases, contact the IND Freedom of Information (FOI) Unit on 0208 760 4658 or 0208 760 4664.

32.1.1. Disclosure of personal information - Outline of legal issues

Of particular relevance where disclosures of personal information are contemplated are common law obligations of confidentiality, the HRA and the DPA, and the administrative law requirement that public bodies must act within the limits of their powers.

Personal information given to the Department by individuals in connection with their applications for leave to enter and remain, asylum, citizenship and humanitarian protection that is not in the public domain may attract an obligation of confidentiality under common law.

A key requirement will be to ensure that not only is the disclosure in pursuit of a legitimate aim but also that the interference with the right is proportionate to the aim. Whether disclosure is proportionate will depend on the circumstances of each case and you should consider proportionality on a case-by-case basis and record your decision so that it can be defended later, if necessary. You should always ensure that any disclosure is not excessive. For example, if the police request a limited amount of information about an individual, it would not be proportionate to respond to that request by sending the police copies of all of the IS files on the individual concerned. The police are only entitled to be told what they need to know for the purpose of their request.

In any case where information is requested from another Government Department, the reason for the request must be ascertained so that you can consider whether disclosure is justified.

For a full explanation of the legal issues see chapter 24 of the IDIs.

32.1.2 Access to Government Information

The 1997 Code of Practice on Access to Government Information has been replaced by the Freedom of Information Act 2000 with effect from January 2005. The Freedom of Information Act 2000 establishes for the first time, for members of the public, a **legal right to know** (subject to exceptions) about information held by public authorities. **See also:**

All public authorities are required to operate the main information access provisions of the Act from 1 January 2005. The Home Office is subject to all of the Act's provisions.

Section 1 of the Freedom of Information Act creates two key information access rights which provide for:

- the right for an applicant to be told whether IND holds the information requested;
- And if that is the case, the right for an applicant to have that information communicated to them by IND.

These two rights in no way discriminate between who can make a request and how a request can be dealt with by IND. Essentially anyone in the world, regardless of their nationality or profession is able to make a request. These rights also apply to information held by IND before 1 January 2005, as well as after this date. A request for information does not even have to refer to the Freedom of Information (FOI) Act for it to be treated under the provisions of the Act itself. Instead, it is the duty of staff to recognise whether a request falls to be dealt with under the Act, and handle it accordingly.

The decision to disclose or withhold information in line with the Act should always be balanced with the need to ensure that this does not affect the integrity or operation of the UK's system of immigration control (subject to exemptions i.e. FOIA section s31 (1) (e)). The approach to release of information should in all cases be based on the assumption that information (but not necessarily the documents in which it was originally contained) should be released except where disclosure would not be in the public interest.

Further details of what the FOI Act requires can be found in chapter 25 of the IDIs.

32.1.3. Disclosure under the Data Protection Act (DPA)

The DPA sets out how bodies, such as the Home Office and IND, who process "personal data" about individuals, should deal with this data. These are known as the data protection principles. The DPA also provides a legal right for an individuals to access data about themselves and to be told what processing goes on and for what purposes (subject to exemptions i.e. DPA section 29). Requests for subject access to personal data made under section 7 of the Data Protection Act 1998 should be forwarded to the Subject Access Bureau as soon as they are received.

There is dedicated guidance for IND staff on the DPA in the IDI Chapter 24.

If an individual refers to the Freedom of Information Act but in fact the request is really for applicants personal data then the request should be sent to the subject access bureau, to be dealt with as a DPA request (under section 40(1) of the Freedom of Information Act).

It is important that data protection principles are respected so that a request under the Freedom of Information Act does not lead to disclosure of personal data about a third party unless that is defensible in DPA terms.

32.2. Disclosure to third parties

The general rule is that any individual or private body, including MPs, other than the subject of an IND personal file or his representative (in which case the DPA subject access request regime would apply), should be regarded as a third party to our records. Information from these records would not therefore generally be disclosed unless there were reasons why it was lawful to do so. In considering whether it is lawful to disclose you will need to consider the legal issues in chapter 24 of the IDIs. This includes requests from former sponsors or representatives and former spouses.

32.2. Applicants/representatives/MPs acting as their representatives

This paragraph concerns requests from the person who is the subject of the data – or people acting on their behalf.

You may provide information about a person to that person where there is no risk that disclosure would prejudice the effective administration of immigration controls or other statutory provisions. You may provide the following:

- copies or summaries of any documents which **they** have submitted in support of an application, including previous correspondence from former representatives (although this should normally be provided by the former representative);
- a record of anything **they** have told us;
- in reports only that part which deals directly with what the applicant has said;
- VAFs and ECO interview notes **provided** they contain no subjective comments.

Before providing the following information, careful consideration should be given as to whether an exemption could be successfully made under the DPA. **These will need to be considered on a case-by-case basis.**

- information about an applicant given in confidence by a third party, e.g. a spouse, without the express and written permission of the informant (subject to exemptions i.e. section 7(4) DPA);
- anything which details our consideration of the facts or other considerations material to the case;
- reports of interviews conducted before 1 October 1985;
- anything subjective, or which deals with the Department's internal arrangements or which offers an opinion or advice to a case-worker;
- Minute sheets, including PEO call-notes (except to confirm details of an application).

32.4. Enquiries from the media – the role of the press office

Refer all enquiries by the media about individual cases to the Press Office (the general public number is 0207 035 4381).

Inform the immigration desk at the Press Office immediately of the enquiry and give the details of the case:

All incidents or stories that have the potential to attract media interest should be reported to Press Office, as well as senior managers, at the earliest opportunity. This includes incidents which local press could consider newsworthy.

32.5. Exchange of information with other government departments

In the light of the 1999 Act, the assumption is that we will exchange information with OGDs, agencies, the police and local authorities subject to relevant data protection requirements and provided the exchange arrangements are properly managed (see IDIs Chapter 24 Section 11), for example, where the information is required to assist with the carrying out of statutory functions or if it is required to prevent or detect a crime.

You should consult the IDIs on disclosure before responding to a request for the information from a third party which includes personal data (information relating to a living individual, including opinions) or information which may be held under a duty of confidentiality. The Data Protection Act 1998, the Human Rights Act and the common law must not be breached. The IDIs will guide you through the steps to be taken in deciding whether the disclosure is fair and lawful in accordance with the Data Protection Act and whether it complies with other relevant requirements of that Act, and if it is not, whether you can rely on any of the exemptions set out in that Act. (The exemptions relate to national security, crime and taxation, and legal compulsion, but do not exempt you from complying with the whole of the Act or with the Human Rights Act). Data Protection and confidentiality policy are co-ordinated by Section 6 IPD.

In deciding whether disclosure is lawful, it should be borne in mind that sections 20 and 21 of the 1999 Act (as amended by section 132 of the 2002 Act) provide a statutory gateway for the exchange of information, documents and articles between the Secretary of State and the police, the National Criminal Intelligence Service (NCIS), the National Crime Squad (NCS), HM Revenue and Customs (HMRC) and a person with whom the Secretary of State has made a contract or other arrangements under section 95 or 98 or a subcontractor of such a person. Sections 95 and 98 refer to the provision of support for asylum seekers and their dependants. However, disclosures made under these sections must still comply with the Data Protection Act, the Human Rights Act, and where applicable, the common law of confidentiality.

Section 20 covers the supply of information, documents and articles to the Secretary of State, for "immigration purposes", by the agencies listed above. It also gives the Secretary of State the power to specify by order further bodies which may supply information to him, and additional purposes for which he may be supplied information, under the section.

"Immigration purposes" means any of the following:

- the administration of immigration control under the Immigration Acts;
- the prevention, detection, investigation or prosecution of criminal offences under those Acts;
- the imposition of penalties or charges under Part II of the 1999 Act;
- The provision of support for asylum seekers and their dependants under Part VI of the 1999 Act.

Section 21 provides for information, documents and articles to be supplied by the Secretary of State to the agencies listed above for specified "purposes". It also provides the Secretary of State with the power to specify by order further purposes for the supply of information to certain of these agencies and other bodies to which information may be provided by him for specified purposes.

Definitions of police, NCIS, NCS and HMCE "purposes" are found in section 21 of the 1999 Act.

Section 20 and 21 are not designed to be comprehensive. As a result, exchanges of information, documents and articles may, to the extent that they are lawful, continue outside the scope of these provisions. Examples of such exchanges are discussed in more detail below.

32.5.1. Department of Work and Pensions (DWP)

As a general rule the DWP are only able to disclose information in the circumstances covered by section 29 of the Data Protection Act (DPA) 1998. Section 29 of the DPA allows an organisation to partially override the provisions of the DPA and provide information to a third party but only when that third party is seeking the information to "prevent or detect a crime". Sections 24(1) (a), (b), (c) and (e), section 24A and section 26(1) (c) of the 1971 Act (as amended) are sufficiently wide to cover the majority of circumstances in which we require information from DWP records.

However, the DPA Act 1998 also adds safeguards so that even if an exchange of information falls within section 29 (prevention of crime), other requirements of the Data Protection Act must be met, in particular satisfaction of conditions at Schedules 2 and 3.

Information may also be disclosed where an individual has given his consent to such disclosure.

A Memorandum of Understanding outlines the circumstances in which information can be sought and disclosed (see IDIs Chapter 24 Section 9 paragraph 2.1 plus Annex A).

The Benefits Agency's Investigation Team can be contacted on weekdays during office hours for benefits enquiries on:

32.5.2. Department of Education and Skills (DfES)

From April 1st 2002 Job Centre Plus took over from Employment Services (ES) and became part of DWP. The Central Point of Contact have access to the records of payment of contributions-based Jobseekers Allowance (JSA) and there should therefore be no need to contact a Job Centre Plus office directly.

32.5.3. Department of Health

The rules of medical confidentiality do not allow for information to be disclosed without the person's permission in any but exceptional circumstances.

32.5.4. Her Majesty's Revenue and Customs (HMRC)

HMRC is statutorily barred from disclosing information to other persons without the consent of the taxpayer concerned, although certain powers of disclosure which override the statutory prohibition have been created (see below). IND has a Memorandum of Understanding for sharing personal data with the HMRC. Staff should contact BIA Intelligence Directorate for further information on the MOU.

Section 130 of the 2002 Act created a new statutory power which allows HMRC to provide information to IND for three specific purposes, provided that certain conditions set out in that section are met. This power came into effect on 1st April 2003. The three purposes are:

- To locate immigration offenders and persons subject to control, working without permission,

- To determine if under the terms of British Nationality Act 1981 an applicant for nationalisation is of "good character", and
- To verify whether sponsored entry clearance applications meet the maintenance and accommodation requirements of the Immigration Rules.

32.5.5. Office for National Statistics (ONS)

Section 24 of the Immigration and Asylum Act 1999 places a statutory duty on Registrars to report marriages which they have reasonable grounds for suspecting to be a sham. For England and Wales the reports are submitted to the BIA Intelligence Directorate (BIA ID) and copied to the General Register Office.

In this connection, a registrar, or the ONS on their behalf, may contact IND for information to establish the details of an individual's identity if they suspect a sham marriage. In such cases it may be appropriate to disclose this information to them; however each case will need to be considered on its own merits, taking into account in particular the requirements of the DPA. The exemption at section 29 of the Data Protection Act 1998 may be relevant in some cases. (A sham marriage is an offence against the Marriage Act 1949 as amended by the Marriage Acts of 1970, 1983 and 1994). Further guidance on the Data Protection Act 1998 can be found in IDIs chapter 24 section 1. All such enquiries should be directed to Business Enquiry Service, Evidence and Enquiry (BES E&E) in writing.

32.5.6. Local authorities

Requests for information from local authorities should be routed through INEB.

There is no central point for obtaining information from local authorities. Approaches may be made to those sections of individual authorities dealing with housing, housing benefit or student awards but not all authorities will be willing to disclose information to IND. In cases where a local authority refuses to comply with a properly made request to disclose information, there is a procedure for requiring certain disclosures under section 129 of the 2002 Act. The statutory request procedure is limited to the obtaining of information for the purpose of locating a person reasonably suspected of having lived in the local authority's area and of having committed an offence either of illegal entry (section 24(1)(a)), overstaying (sections 24(1)(b)(i) and 24(1)(c), failing to observe a condition of leave or temporary admission (including restrictions imposed under Schedule 3 of the 1971 Act) (under sections 24(1)(b)(ii) and 24(1)(e), disembarking from removal (section 24(1)(f)), deception

(section 24A(1)), making false representations to an Immigration Officer section 26(1)(c)) or creating or possessing false documentation (section 26(1)(d)). Further guidance on the operation of this procedure is now contained in the IDIs chapter 24 section 3.

32.5.7. Information requests that should be referred to INEB

Most requests for information should be referred to INEB e.g. from the police, HM Customs and Excise, Institutions of Higher and Further Education or the Universities and Colleges Admissions Service (UCAS).

When you make enquiries of other bodies, you should make it clear who you are, where you are based and the reason for the enquiry. You should also make it clear that the approach is an official one and that any information received will be treated as having been officially obtained from the source. You should not enter into personal unofficial arrangements with individuals in other agencies or where an agency expresses a reluctance to disclose information.

The 2002 Act also contains provision at section 134 for requiring information from employers, similar to that applying to financial institutions, but this is a wider power than that at section 135 (chapter 32.6).

32.5.8. Information from police

When the police have in custody a person whose immigration status is in doubt, they will seek the assistance of the IS. You must attempt to resolve the person's status by the standard checks (see chapter 31.3).

Section 20 and 21 of the 1999 Act (as amended by section 132 of the 2002 Act) provide a statutory gateway for the exchange of information, documents and articles between the Secretary of State, the police and various other agencies. Chapter 32.5 contains a more detailed explanation and should be referred to if further details are required.

When an IO attends a police station in order to ascertain the immigration status of a person in police detention, the PACE safeguards apply and the responsibility for the welfare of that person rests with the police (and in particular the custody officer). Only if and when the person is released from police detention and action is then taken under Schedule 2 of the 1971 Act to detain the person is detention the responsibility of the IS.

32.6. Information from Banks, Building Societies and Credit Card Companies

These have a duty of confidentiality to their customers and they should not be approached for information. The exception is where it is reasonably suspected that (i) a person has committed a specified offence, (ii) the information is relevant to the offence, and (iii) the financial institution in question has the relevant information (see section 135 of the 2002 Act). The specified offences for the purposes of section 135 of the 2002 Act are under section 105(1) (a), (b) and (c) and 106(1) (a), (b) and (c) of the 1999 Act. These offences relate to defrauding NASS. "Financial Institution" is defined in section 135(2) of the 2002 Act.

In those cases a procedure has come into force under section 136 of the 2002 Act whereby a statutory notice must be served on the institution requiring it to provide specified information relevant to the offence within a set period. Failure to comply with such a notice without reasonable excuse is punishable with a maximum penalty of three months' imprisonment, a fine not exceeding level 5 on the standard scale (currently £5,000) or both.

32.7. Denunciations received in enforcement offices

Any allegation received in an operational enforcement office should be passed immediately to the intelligence unit for processing. The information will be passed back for action by operational teams once it has been sanitised in the form of an intelligence report. This process will prevent inadvertent disclosure of the source of the denunciatory information.

Where possible denunciatory phone calls should be transferred to the intelligence unit however if this is not possible or practicable you should record the information yourself and pass it immediately to the intelligence unit. When taking denunciatory information over the telephone be aware of the possibility that the person may be a Covert Human Intelligence Source (see chapter 32.8.3). You may ask as many questions as you like about the information they have and in some circumstances even ask them to gather more so long as this does not involve their establishing or maintaining a relationship for the covert purpose of obtaining or providing access to any information or disclosing information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. For example if they are telling you about someone they saw by looking out of their window, there is no reason why you cannot ask them to have another look to see if they are still there as there is no relationship involved. However they should not be asked or encouraged to go and introduce themselves to covertly find out what the person is doing there. By doing so they are

establishing a relationship and making themselves a "CHIS". If in doubt speak to your local intelligence manager or to BIA Intelligence Directorate.

You should never act on un-sanitised denunciatory information as there is an increased chance that the identity of the source, which we have a duty of care to protect, will be revealed. Only in highly unusual circumstances should you consider doing so such as where there is a genuine threat to a person's safety or liberty.

32.8. The Regulation of Investigatory Powers Act

The Regulation of Investigatory Powers Act received Royal Assent on 28 July 2000. The Act updates the law on the interception of communications to take account of technological change such as the growth of the Internet. It also puts other intrusive investigative techniques such as covert surveillance and covert human sources on a statutory footing, provides new powers to help combat the threat posed by rising criminal use of strong encryption and ensures that there is independent judicial oversight of the powers in the Act.

Part II of the Act, which covers covert surveillance and covert human sources, came into force on 25 September 2000. The Statutory Codes governing the exercise and performance of the powers in Part II of the Act have been brought into force by the following regulations:

I. The Regulation of Investigatory Powers (Covert Surveillance: Code of Practice) Order 2002 – bringing into force the Code entitled "Covert Surveillance"

II. The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Code of Practice) Order 2002 – bringing into force the Code entitled "Covert Human Intelligence Sources"

Both Codes came into force on 1st August 2002. Copies of the Codes can be found on the Home Office web-site at www.homeoffice.gov.uk/ripa/ripact.htm.

32.8.1. Surveillance under the Regulation of Investigatory Powers Act

"Covert surveillance" is covered in the Act in two areas - **directed** and **intrusive**. Only "covert" surveillance is covered by the Act. Surveillance is covert if it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be

taking place. The Act does not regulate general observation in public, for example, at ports, where this **does not** involve systematic surveillance of an individual. Such general observation is regarded as forming part of the everyday functions of law enforcement and other public bodies. It will not restrict officers from placing and keeping under observation individuals who come to their attention in the normal course of their duty and who are suspected of having committed or being about to commit offences. Nor does the Act cover authorisation for the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. However, where CCTV is used as part of a pre-planned operation or investigation RIPA does apply. The Act, and related Codes of Practice, covers the deployment of vehicle and foot surveillance personnel, the setting up of covert observation posts and the installation of equipment for covert, remote, monitoring of specified or unspecified individuals in public places.

'**Directed**' surveillance is defined in sect 26(2) of the 2000 Act as surveillance which is covert, but not intrusive, and is undertaken:

- for the purposes of a specific operation or investigation; and
- in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
- otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the Act to be sought for the carrying out of the surveillance.

'**Intrusive**' surveillance is defined in sect 26(3) of the 2000 Act as surveillance that is covert and:

- is carried out in relation to anything taking place on any residential premises or in any private vehicle, and
- Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Surveillance is NOT intrusive where it is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle, but is carried out without the device being present on the premises or in the vehicle, UNLESS the device is such that it

consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

32.8.3. Covert Human Sources

The legislation puts the registration and tasking of covert human sources (informants, agents and undercover operatives) on a statutory footing. Codes of Practice regulate their management, authorisation for their deployment and the training of informant/agent handlers.

Members of the public who give information to assist law enforcement agencies once or on occasions and expect nothing in return are not classified as informants. The Act is not intended to regulate the flow of information, anonymous, denunciatory, public-spirited or otherwise or the passage of information from business contacts or other departments who may suspect criminal activity. This type of information exchange is covered by Data Protection legislation and other statutory legislative frameworks.

A covert human intelligence source is defined as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating the doing of anything falling within either of the following two paragraphs:

(a) He covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(b) He covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

32.8.4. Impact of the Regulation of Investigatory Powers Acton the Immigration Service

The IS is empowered under the legislation to authorise the use of:

- directed surveillance; and
- Covert human sources.

<u>For the following purposes only:</u>

- For the purpose of preventing or detecting crime or of preventing disorder.

- The economic well-being of the United Kingdom.

The IS has no authority to authorise the use of intrusive surveillance.

The general level for authorising directed surveillance and covert human sources will be at Immigration Inspector grade but there will be certain categories where authority will be required at Director or Senior Director level. SEOs and other non-warranted grades in the Immigration Service are not empowered to act as authorising officers.

BIA Intelligence Directorate has conducted a program of RIPA awareness training and the subject is now included on all enforcement induction and conversion training but anyone who is unsure if proposed activity falls within the scope of RIPA should contact BIA Intelligence Directorate for advice before commencing.

It is current policy not to use CHIS until the correct infrastructure; training and expertise are in place. In the interim no CHIS is to be run by the Immigration Service. Work is currently underway to establish Dedicated Source Handling Units (DSHU) but this work will take considerable time to realise benefits. In the interim a number of IS officers around the country have undergone Source Handling training and there are already some agreements in place locally with certain agencies and police services to allow for CHIS to be cultivated and deployed for immigration purposes. However these are run under the management of the agency or police concerned and not by the IS. All such arrangements are authorised and controlled centrally and any potential CHIS should be referred to BIA Intelligence Directorate. All source handling training must be arranged through BIA Intelligence Directorate.

Under no circumstances should staff recruit, cultivate or deploy a covert human source. Any member of staff who seeks to cultivate or deploy CHIS is liable to disciplinary action and potential legal challenge.

IS policy on directed surveillance is that no such activity should be conducted unless the staff involved have been trained to ACPO level 2 standards. All such training must be arranged by BIA Intelligence Directorate. Directed Surveillance should only be conducted once it has been approved by an authorising officer of at least substantive HMI rank. In cases where the HMI is unavailable, urgent oral authority can be obtained from an authorising officer of least substantive CIO. No

member of staff should conduct directed surveillance without appropriate authorisation having been given by an authorising officer. Authorising officers will also be responsible for ensuring that all officers deployed on covert surveillance operations are appropriately trained and accredited. BIA Intelligence Directorate run periodic courses to train officers of CIO and HMI rank to act as authorising officers. Only those officers who have been trained and appear on the BIA Intelligence Directorate list should sign off authorities. If any officer is unsure whether they appear on the list they should contact BIA Intelligence Directorate for clarification. Under no circumstances should any member of staff serving in IS ever undertake intrusive surveillance.