The following table accompanies the 2005-2010 redacted version of the GCHQ Compliance Guide. As it is not possible to gist within that document, only redact, this table contains alternative text.

(Internal) Page/paragraph number	Gist
Page 15, para 9	'foreign partners'
Page 15, footnote 2	'It is essential also for GCHQ staff, in their conduct to respect the sensitivities of liaison countries as they respect ours. Consultation with foreign liaison partners will ensure that they cannot be compromised by receiving from GCHQ material which they could not legally collect for themselves.'
Page 31, paragraph 8	'Except in the cases of collaborating SIGINT liaison partners, information is normally issued to customers outside GCHQ only by way of formal intelligence report.'
Page 31, paragraph 9	'E.g. liaison partners'
Page 32, paragraph 12	'Change of ownership is particularly important to record where ownership moves from GCHQ to liaison partners'.
Page 137, paragraph 10	'Duty Officer'
Page 163, paragraph 4	'intelligence'
Page 199, paragraph 1	'requirement'
Page 199, paragraph 3 Q2	If a Sensitive Targeting Authorisation (STA) required for the target, has STA been obtained (given that a RIPA warrant is not required)? If so, does this targeting relate sensibly to its terms?
Page 200, bullet 1	'requirement'
Page 200, bullet 4	'database'
Page 200, paragraph 5 b	'the relevant database'
Page 200, paragraph 5 c	'database'
Page 201, paragraph 10	'The relevant GCHQ senior officials and Legal Advisors'
Page 213, paragraph 8	'The relevant GCHQ senior officials and Legal Advisors'
Page 217, paragraph 6	'intelligence reporting'

The Human Rights Act 1998

1. The Human Rights Act 1998 (HRA) incorporates into UK law the main rights contained in the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (ECHR).

2. Article 8 ECHR is of particular relevance to the work of GCHQ[1]:

   '1. Everyone has the right to respect for his private and family life, his home and his correspondence'.

3. Just as important are the circumstances in which certain ECHR rights might be limited justifiably in a democratic society (so-called "derogations"). Article 8, paragraph 2 contains such derogations:

   '2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others.'

4. In order to justify any interference with these rights, a public authority must be able to demonstrate that the interference:

   - **is prescribed by the law**
     - achieved if GCHQ operations comply with the Regulation of Investigatory Powers Act 2000, the Wireless Telegraphy Act 1949 and ISA;
   - **has an aim which is legitimate under Article 8, paragraph 2**
     - achieved if GCHQ's operations have, as their legitimate aim, one or more of the authorised purposes (which appear also in Article 8, paragraph 2);
   - **is necessary in a democratic society**

[1] Article 10 rights (Freedom of Expression) are couched in terms that are similar to Article 8. Article 6 (Right to a Fair Trial) has a potential impact where GCHQ has produced intelligence of potential relevance to court proceedings, *e.g.* in support of the prevention or detection of serious crime, or in the interests of national security (especially counter-proliferation or counter-terrorism activities).

- the necessary interference must be convincingly established and proportionate to the 'legitimate aim' being pursued;
- the reasons given in justification must be both relevant and sufficient

The Concept of Proportionality

5. While a public authority should not be unduly restricted in what it is trying to achieve legitimately, GCHQ's actions must constitute a proportionate means of securing achievement. In the first place, this means that, if other methods are available and these methods are equally effective but less intrusive, then the customer is bound to have considered these beforehand[1]. Where action by GCHQ is the most appropriate method, it must be implemented with the minimum interference with Convention rights in so far as the demands of the intelligence requirement and the knowledge available to GCHQ allow.

6. In GCHQ terms, for instance, the selectors used to target an individual must retrieve the least possible material to satisfy the requirement, and the output should be reviewed periodically to ensure that this is so. It means also observing the 'minimisation' procedures with regard to copying, dissemination and retention, given in **SECTION VI.**

Main Responsibilities Imposed by the HRA

7. The HRA charges all public authorities in the UK with a responsibility to act compatibly with the Convention rights. The Act does not prescribe how this should be done, so it is largely a matter of policy within each Public Authority as to how this is achieved.

8. Because the potential effect of HRA is so wide, and because most SIGINT operations have an obvious potential to infringe someone's privacy, GCHQ's established policy is that every aspect of every GCHQ operation must conform to the principles expounded above[2].

[1] GCHQ may still confer a benefit on the basis of economies of scale, timeliness, etc. where the relative advantages of different courses of action are not clear-cut. Where the arguments against GCHQ action are obvious, the tasks must be refused.

[2] This assumes that HRA rights have extra-territorial effect, which is consistent with the advice given by the Attorney-General and The Law Officers before the HRA came into effect.

9. Some form of legal authorisation for GCHQ's work (carried out at any facility in the UK or abroad) is required in respect of work against all individuals and organisations (except governments and military forces[1]), regardless of their nationality. We have to manage also the HRA implications of work carried out on behalf of our [redacted] at any facility in the UK owned by GCHQ, or controlled by GCHQ. This includes any requests made to, or by, other Agencies or organisations for material[2].

10. Staff may assume that, by acting in accordance with the guidance given here, they will ensure that GCHQ does not act in a manner that is inconsistent with the rights guaranteed under the HRA. The provisions of RIPA and ISA, to which GCHQ's operations are also subject, are designed to comply with the demands of the Convention.

[1] The Convention does not establish a right to privacy on behalf of the public authorities of other countries, only their citizens. Nevertheless, UK law might still require a RIPA interception warrant to be acquired, for example, in respect of a diplomatic mission located in the UK.

[2] [redacted]

The Regulation of Investigatory Powers Act 2000

1. The Regulation of Investigatory Powers Act 2000 (RIPA) ensures that certain intrusive surveillance powers are used in accordance with human rights legislation. It covers the purposes for which these powers may be used and what authority is required before each use.

2. **Part I of RIPA** covers the interception of communications (including monitoring for lawful business purposes, such as INFOSEC, COMSEC monitoring/penetration testing), and the acquisition of communications data: see **Annex B: Communications Data.**

3. **Part II** provides a scheme for the authorisation of directed or intrusive surveillance and for the operation of "Covert Human Intelligence Sources" ("CHIS")[1]. This allows for activities that aim to obtain information about an individual: **see Annex C: Covert Surveillance).** To the extent that GCHQ's activities might fall within the rest of Part II RIPA (e.g. contacts with industry): see **Annex D: Sensitive Contact Management.**

4. **Part III** (not yet enacted) provides for powers concerning electronic data protected by encryption: **see Annex E: Disclosure of Encryption Keys.**

Main Responsibilities imposed by RIPA

5. Where authorisations are required under RIPA, GCHQ operations cannot go ahead without those authorisations being obtained beforehand.

6. The Act also regulates the use that can be made of the material acquired under RIPA. Sections 15 and 16 of RIPA require the Secretary of State to be assured that arrangements ("safeguards") are in place to achieve this aim, before any RIPA warrants are issued to a Department. The Compliance documentation as a whole constitutes the safeguards for the purposes of GCHQ. They have been approved as such by the Foreign & Commonwealth Office (**➲ 3**).

[1] Where GCHQ is acting under the authority of an interception warrant issued under Part I of RIPA - which it will be doing in the majority of cases - then no further consideration needs to be given to Part II. However, other activities within GCHQ's remit under the ISA may do so (even those authorised by an ISA warrant).

7. For the purposes of GCHQ staff, this guidance provides material additional to the Codes of Practice published by the Home Office pursuant to section 71 of RIPA and effective from 01 July 2002. This guidance should be used by GCHQ production analysts as the primary source of information about the law. Any apparent inconsistency with the Codes of Practice should be reported to the Operational Legalities Branch (➲ 2)

Other Legislation

8. This list is not exhaustive. Other legislation, where relevant, may be mentioned in the body of the text.

CROSS REFERENCES:
➲ 1. "Interception Of Communications: Code Of Practice" (to be made available on GCWeb)
➲ 2. Operational Legalities Branch [redacted]
➲ SECTION VI: SAFEGUARDS

Special Responsibilities for Compliance: The Responsibilities of Reporters and Analysts

Targeting

1. The analyst who requests, or causes, a Targeting selector to be implemented (whether for production or SD purposes) 'owns' that selector[1]. It is the 'owner's' responsibility to demonstrate compliance with all legislation, including the Human Rights Act (HRA).

2. Any authorisations received under RIPA will automatically comply with the HRA. But all targeting implemented on GCHQ systems still requires three categories of information that are mandatory (➲ 5):

   - **the intelligence requirement,** [redacted]
   - the **JIC Priority** and the **'authorised' purpose** of the requirement, *i.e.* in the interests of national security, to safeguard the economic wellbeing (EWB) of the UK, or for the prevention or detection of serious crime (➲ 4)
   - **the HRA justification for the targeting,** *i.e.* how the Targeting of this selector contributes reasonably to meeting the intelligence requirement(s) ('proportionality'). This does not equate to the intelligence requirement but explains why and how that requirement is being met by that targeting. That said, the link to the requirement might be self-evident from an official's position, or a ministry or agency name.

3. Where the link between intelligence requirement and the target or selector is not immediately obvious, there should be a brief description of the justification, supported by a link to a documentary audit trail which will allow further supporting information to be provided quickly and easily[2]. This should allow GCHQ to respond to any complaint made to the Investigatory Powers Tribunal under RIPA/HRA.

[1] [redacted]

4. [redacted]

5. Reporters and analysts have responsibility for checking that any tasking or selection terms which they have originated are in fact producing output proportionate to their intelligence requirement. Any tasking or selection which is not should be refined or deleted immediately. If such tasking or selection has constituted a breach of RIPA or the ISA, or of the safeguards associated with those Acts, the matter **must** be reported to line management for action (⛔ 1).

6. [redacted]

7. Where queries are made to databases containing intercepted material, HRA justification related fields must be filled in, using the guidelines given above. The systems will also automatically create an audit trail which can be used by GCHQ to respond to complaints received under the HRA. Queries which are designed merely to retrieve specific targeted traffic [redacted]

[redacted]

The disclosure of information

8. The role and responsibilities of reporters and analysts are of central importance to the disclosure of information which has been acquired by GCHQ. [redacted].

9. In this way, GCHQ analysts and reporters release information:

   - to **UK recipients** in order to satisfy HMG requirements;
   - to **non-UK recipients** [redacted] to satisfy their requirements.

   In each case, this release must be for necessary for one or more of the purposes authorised under ISA, *i.e.* in the interests of **national security** or the **economic well-being** of the UK (the actions or intentions of persons outside the British Islands), or in support of the prevention or detection of **serious crime** (⊖ 2).

10. The report content must also observe the principle of proportionality in disclosing information only to the minimum extent necessary to satisfy the intelligence requirement, especially with regard to the amount of information disclosed and the level of detail that is provided. GCHQ analysts and reporters must also take care not to disclose certain categories of information at all, or to disclose it only after consultation and/or with special handling instructions (⊖ 3).

[1] Information may also be provided by GCHQ to customers in some other approved manner, [redacted]

Revalidation of selectors

11. Targeting selectors, and their HRA justification, need to be revalidated periodically. As a rule of thumb, the less discriminatory a selector is, the more frequently it will need to be revalidated. It is a vital measure of proportionality that selectors will return a reasonable quantity and quality of material that is likely to serve the intelligence requirement. (This cannot be measured in absolute terms: one item returned in any one year might justify the selector in itself; several low-level items of only marginal interest might require that selector to be removed). Similarly, selectors relating to particularly volatile or sensitive targets will need to be revalidated more often. A conscious (and justifiable) decision is required with the fundamental question being: *"is this reasonable and proportionate?"* As a maximum default selectors need to be reviewed annually (3 months for SD selectors).

12. The requirements for accurate and efficient response to any complaints made to the Tribunal are such that we will need to know whether a selector was on task during the period to which a complaint refers and for what reason it was tasked. The period covered by a complaint could be current or historical[1] (or since such-and-such a date and continuing). This means that for all changes that are subsequently made to a selector's ownership, tasking and justification and also the dates on which any changes are made **must** be recorded.

[redacted]

The Responsibilities Of Line Managers For Audit

13. All database queries are recorded permanently by means of an automatic audit trail to which the date of the request and the name of the analyst responsible is appended; at intervals, line managers in areas where staff require access to the databases will review samples of the audit trails to check

[1] Historical complaints cannot, however, pre-date the introduction of the HRA into UK law (2 October 2000).

- that queries are being formulated according to best practice (especially with regard to 'proportionality');
- that proper authorisation procedures are being observed;
- that all queries can be accredited to a purpose allowed to GCHQ by the legislation.

Improper use or bad practice will be detected and deterred by this procedure.

CROSS REFERENCES
1 General; Responsibility for Compliance
2 General; GCHQ's Purposes
3 SAFEGUARDS; The Intelligence Services Act, 1994 and Human Rights Act, 1998: Recording and Reporting Confidential Information
4. General; Main Statutory Responsibilities Discharged by this Guidance; the Human Rights Act 1998

Procedure to follow where communications are intercepted without the necessary authorisation

1. Where, despite the taking of all reasonable care, communications which fall within the provisions of the Act are intercepted inadvertently, and without the necessary authorisation, GCHQ staff must apply the following procedure at once:

   (a) **interception must cease** as soon as the nature of the communication is identified (where interception is still in progress);

   (b) **any copies of any recording must be destroyed.** All recipients of the material must be notified and told to act similarly. (The original only should be retained until legal advice has been received regarding its retention or destruction);

   (c) **technical details should be recorded** to a level of detail sufficient that inadvertent interception of the same communications is avoided in the future (and no more)[1];

   (d) **the incident must be reported to line management,** and, through them, to the Operational Legalities Branch. They will involve the Legal Adviser and the tasking authority (if relevant), investigate the circumstances and report to Directorate (➲ 2).

2. There may be borderline cases. Any current operation about which there is genuine doubt should be referred to line management for action in accordance with the prescribed procedures (➲ 3).

CROSS REFERENCES
➲ 1. The Regulation of Investigatory Powers Act 2000: What communications are covered?
➲ 2. Operational Legalities Branch [redacted]
➲ 3. General; Responsibility For Compliance

[1] In no case should interception be continued to establish or confirm technical details; staff should record whatever is available and continue with their proper monitoring task.

'Communication'

1. A distinction is drawn between 'subscriber communications' and 'communications data'. This distinction does not depend upon which mode of the system is used to carry the data in question (so 'content' that is carried in a 'signalling' channel remains content for the purposes of the Act).

Subscriber Communications

2. The term '**communication**' is not defined in the Act. It is held to be a signal which conveys information through content. The notion of what constitutes content must be construed widely[1]. Any information which is generated by the sender or recipient of a communication is assumed to be content, regardless of whether it is speech or not:

    - voice mail boxes, Short Message System (SMS) text ('text messaging'), *etc.* are all subscriber communications regardless of the part of the system which is used to convey them, or to store them[2].
    - non-speech signals (e.g. DTMF tones transmitted by means of the sender's keypad) may also qualify as subscriber communications. This is true even if such signals are being filtered from out of a subscriber channel, and the speech in that channel is being discarded.

3. Where it is not possible technically to intercept communications data without, at the same time, having access to subscriber communications in the same channel, that channel must be treated as if it were carrying subscriber communications, and the appropriate authorisation(s) obtained. (See also the advice given in paragraph 5 below).

---

1 The House of Lords has ruled that '*it is sufficient [...] for an electrical impulse or signal to be transmitted from the telephone number from which the impulse or signal is sent to the telephone number with which it has been connected [...] irrespective of the response which it elicits from the recipient and the length or content of the message which it conveys*': Lord Hope of Craighead in ***Morgans v. DPP*** [2001] 1 A.C. 315, HL(E.), at 333C.

2 A communication is also in the course of its transmission when it is stored on a communications system in such a way that the intended recipient has access to it: *section 2(7), RIPA*. These data may be accessed by a RIPA warrant, a search warrant or production order, *etc.*

Communications Data

4. RIPA defines 'communications data' to mean *'(a) traffic data attached to a communication for the purposes of the service provider, (b) any non-contents information regarding the use made of a service by a person, or (c) any other information held about a person to whom a service is provided' (sub-section 21(4)).* The subject of communications data (including the requirements placed upon analysts by RIPA regarding their acquisition) is dealt with elsewhere, in **Annex B: Communications Data.**

5. The definition of interception used for the purposes of RIPA does not include the collection only of communications data, or traffic data, as defined in paragraph 4 above. However, if, in order to obtain traffic data, it is necessary to scan through other material, such as SMS messages in a 'signalling' channel, a decision as to whether that constitutes interception or not would depend upon whether the extraneous (non traffic) data was discarded at the earliest stage possible, without being intercepted within the meaning of the Act, and whether the procedures for doing so were recorded. Nevertheless, such scenarios obviously exist in the shadows of the advice given here, and anybody contemplating such actions would be advised to consult with the Legal Policy branch or with Legal Advisers before proceeding.

RIPA warrants

1. RIPA provides for two kinds of warrant.

A. Warrants for 'internal' communications

2. In accordance with *section 8(1) RIPA*, a warrant can be issued to authorise the interception of **'internal'** communications, *i.e.* communications between any two points in the British Islands (➲ 1).

3. This comprises:

   - the **warrant**, which authorises interception against the individual or premises named, and;
   - one or more **schedules**, which list the selection factors (addresses, numbers, apparatus, *etc.*) that will be used to identify the communications to be intercepted[1].

4. The warrant is addressed back to the organisation which has applied for it; schedules are addressed to those who can provide the intercepted material to that organsiation. It is possible, therefore, for a customer organisation to obtain a RIPA warrant and to address a schedule to GCHQ (if interception by GCHQ is a necessary and proportionate means of obtaining the communications). Intercepted material may also be 'dual-routed' (*i.e.* supplied to another organisation in addition to the applicant) in cases where the second organisation may add value or benefit. For example, GCHQ's expertise may be required to demodulate a complex signal or to translate an obscure language or dialect. This is regarded as an administrative measure to be arranged between the supplier of the intercept, the applicant organisation and the second organisation.

CROSS REFERENCES
➲ 1. Communications; 'internal' communications

1 Schedules may be modified by a senior official in the department of a Secretary of State, without each modification being referred to the Secretary of State personally.

B. Warrants for 'external' communications

5. In accordance with **section 8(4) RIPA**, a warrant can be issued to authorise the interception of 'external' communications, *i.e.* communications sent and/or received outside the British Islands[1], that are carried on any part of the Global Telecommunications Network and which connect **into** a UK public or private network or are relayed **from** a UK public or private network[2].

6. The provisions of such a warrant comprise:

   - the **warrant**, which authorises the interception of 'external' communications, and;
   - a **certificate**, which describes the intelligence requirements to be satisfied by examining the intercepted material[3].

7. Special rules govern the **selection** of communications relating to individuals located in the UK where those communications have been **intercepted** under the authority of an 'external' warrant. The **interception** of these communications is authorised by the warrant under section 8(4) but their **selection** must be authorised by a certification in accordance with sub-section 16(3) of RIPA, or by a separate warrant under section 8(1).

8. In order to intercept the communications specified by an 'external' warrant, it may be necessary also to intercept other communications. Even though some of these 'other' communications may be 'internal', a warrant issued in accordance with section 8(4) authorises their interception also, but only to the extent that their interception is necessary in order to effect the 8(4) warrant, and their presence cannot be diagnosed beforehand[4].

---

1 One end of the link **must** be outside the British Islands; the other end **may** often be in the UK.

2 GCHQ also obtains a RIPA warrant to authorise the interception of 'external' communications that are carried on any parts of the global telecommunications network (radio or satellite systems) whether they are located in the UK or outside, and on non-governmental (foreign) private networks, *e.g.* merchant shipping communications. Although the interception of such communications would fall outside the **criminal** offence established by RIPA, GCHQ obtains a RIPA warrant as a matter of policy to secure **HRA compliance**. (The Attorney General's advice is that UK public authorities should act in accordance with the HRA wherever the effects of their conduct might be felt). RIPA safeguards will apply to all material intercepted under this warrant.

3 Examination' customarily occurs when GCHQ analysts translate these approved requirements into selection factors which are applied to the intercepted material.

4 *Sub-section 5(6) of RIPA* applies, *viz. 'The conduct authorised by an interception warrant*

[redacted]

shall be taken to include- (a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant, etc.' Of course, where the prior *intention* is to intercept directly the communications of an individual known to be located in the British Islands, then paragraph 7 applies in all circumstances.

[redacted]

Communications associated with individuals located in the UK

6. Where a search relates to stored intercepted content associated with a person located in the British Islands at the time of the search, STA must be obtained first from a member of Directorate. STA authorisations must cover the dates on which the search(es) are actually conducted rather than the dates of interception.

7. Authorisations obtained under Part I or Part II of RIPA or under the ISA also permit the subsequent searching of any material intercepted under their authority[1]. The approval(s) relate to the time frame of the intercepted material to be searched. Where the RIPA or ISA authorisation does not cover the whole period of the searches, STA will still be required for the period that is left unauthorised by RIPA.

8. The warrants may have been issued to GCHQ or to a collaborating agency, although, in the latter case, GCHQ must be careful to act only after a copy of the authorisation has been obtained. For comfort, analysts may consider it wise to obtain STA from Directorate in these circumstances, using the warrant as supporting evidence.

STA and the data mining of content

9. For targets located outside the UK, STA procedures must be observed, and any authorisations obtained **before** you submit the query **(➲ 3)**.

10. Note that, as with travel tracking (below), authorisation under STA depends upon GCHQ's state of knowledge regarding where the target is located now rather than at the time of intercept (which could be a laborious and ultimately pointless exercise). If you have any queries, contact your divisional co-ordinator, or the Operational Legalities Branch **(➲ 4)**.

B. Communications Data

11. No authorisation is required to access communications data (once it has been acquired) but full justification and proportionality criteria must be observed when reporting the output.

[1] The warrants will have authorised all necessary actions taken later in relation to the intercepted material.

SECTION IV: SIGINT Development

The Scope of SIGINT Development

1. The term 'SIGINT Development ' (SD) is used to denote a diverse range of activities which all share the aim of developing (rather than exploiting) SIGINT capability. Without SD, sustained SIGINT collection would become impossible so, in addition to collection directed against specific target emissions, it is necessary for GCHQ to research in a more general way:-

    - to determine what emissions may be available for collection, or;
    - to identify wanted target communications from amongst those known to be available.

2. Typically, this is an iterative process. The end point will always be defined[1]; the starting point will depend upon the nature (and ultimate aim) of the task, and the state of the knowledge available to GCHQ at any one point. Subject to the requirements of proportionality[2], SD tasking might be initiated by simple, occasionally broad, parameters which nevertheless represent the most effective way of ultimately identifying traffic belonging to the wanted targets. As the analyst's knowledge increases, the initial parameters will be refined or logically combined with further, more sophisticated, ones. At the end of the process, any selectors used for sustained collection and reporting will be justified in the usual terms before being applied.

The Effect of Legislation on SD

The Regulation of Investigatory Powers Act 2000

3. RIPA provides for warrants to be issued to intercept either 'internal' communications (section 8(1)) or 'external' communications (section 8(4)). Where 'external' communications are intercepted, 'extra' safeguards must be in place to ensure that intercepted material is read, looked at or listened to by any person only to the extent that is authorised by the accompanying certificate.

---

[1] This may not be in terms of a specific target but may refer, e.g. to required target communications (of a type either known or reasonably expected to be used by a specific intelligence target) or to required target activity (such as hacking or fraud). Justifications may also be framed in terms of maintaining GCHQ's technical knowledge, which serves the national security purpose of preserving the UK's SIGINT capability.

[2] See below under **The Human Rights Act 1998.**

4. The certificate issued to GCHQ allows for the examination of previously unexamined messages for SD purposes but this must be done only within the policy constraints given in this section of the guidance (➡ 1).

The Intelligence Services Act 1994

5. Where RIPA does not apply, SD, as with any other SIGINT activity, must be conducted only for one (or more) of the three 'authorised' purposes: in the interests of the national security, or of the economic well being, of the UK, or in support of the prevention or detection of serious crime.

The Human Rights Act 1998

6. To ensure consistency with the Human Rights Act, any activity by GCHQ (including SD) must be in accordance with the law, *i.e.* RIPA, or where it does not apply, the ISA.

7. It must also be proportionate (*'necessary in a democratic society'*), especially

   - the terms in which collection and/or selection are formulated for a SD purpose must be restricted to the minimum necessary in order to achieve that purpose[1], and;
   - the (short) **length of time** and the (limited) **amount of data** collected in the period (which must be the minimum that is necessary in order to achieve the established aim)[2], and;
   - the criteria used to determine when to move on to sustained targeting, and;
   - strong **safeguards** which relate to the dissemination and retention (or destruction) of the material so collected.

[1] For example, it would not be proportionate to target all of an ISP's communications simply because a key target uses that ISP, but (for SD purposes) it might be proportionate to target all IPs on an ISP for a short enough time to establish whether there were any users or target activity likely to meet an intelligence requirement. The key to proportionality in this circumstance would be the restriction imposed on the size of the sample, and the length of time for which SD is conducted before selection terms are refined, and the safeguards developed for handling the material.

[2] Where an SD task has gone beyond its original time limit, it should be specified anew, using knowledge acquired to date, and should contain an assessment of what is left to be done, and how long that will take.

Proportionality

8. Proportionality should be assessed continuously and on a case-by-case basis. For instance, there is likely to be a limit to the number of times that unfiltered or crudely-filtered interception could be conducted for SD purposes. This is because you might be expected to learn something new about your target and the communications environment every time you sample, and you would be expected to apply that to subsequent activities[1]. At the other end of the scale, it could be justifiable to target an individual under an SD heading if, for instance, you were not interested in the individual so much as specialist information he might (or might not) have which would enable GCHQ to refine its targeting or to expand its range of intelligence techniques.

9. [redacted]

CROSS REFERENCE

⊖ 1. SAFEGUARDS; 'Extra' safeguards required by section 16 RIPA; the examination of material that has not been selected for a specific certified purpose

[1] [redacted]

SECTION VI – SAFEGUARDS REQUIRED BY THE ISA, HRA and RIPA

Safeguards required by the Intelligence Services Act, 1994

1. **The Intelligence Services Act of 1994** (ISA) requires Director GCHQ to ensure that arrangements exist so that information is obtained or disclosed by GCHQ only so far as is necessary for the proper discharge of its functions. Director GCHQ has approved these safeguards, which apply to all SIGINT operations under his control.

2. The safeguards required by the ISA are applied in the following way:

   - **the acquisition of information** from communications and other emissions is controlled by authorisation procedures[1] (➡ 1), and;
   - **the creation and keeping of records**, for intelligence purposes, of information about individuals and organisations must be limited to justified and proportionate circumstances[2], and;
   - **the reporting and other release of SIGINT** must also be limited to justified and proportionate circumstances.[3] (➡ 2).

[1] Since GCHQ acquires information exclusively through the monitoring of or interference with emissions, the arrangements made for interception constitutes the first stage in the creation of a record.

[2] These records might take the form of SIGINT raw material, extracts from this material (including [redacted] (intelligence) reports), and non-SIGINT material obtained by GCHQ to aid its own intelligence production. Records kept and maintained for targeting purposes or to build personality profiles of targets are also included. GCHQ may use such information negatively, *i.e.* to ensure that material referring to certain persons is **not** retained or reported; this category of information is not included.

[3] As a matter of GCHQ policy, all intercepted material is handled and released as though it had been intercepted under a RIPA warrant.

Safeguards required by the Human Rights Act, 1998

1. **The Human Rights Act of 1998** (HRA) imposes obligations on public authorities to act in a manner that is not inconsistent with the ECHR. (GCHQ is a 'public authority' within the meaning of the Act).

2. Compliance with the HRA is achieved through compliance with the ISA and with RIPA, and by applying the principles of justification and proportionality to all stages of the intelligence production process. To that extent, there is no need to consider safeguards additional to those appearing here.

Safeguards required by the Regulation of Investigatory Powers Act 2000

1. **The Regulation of Investigatory Powers Act 2000** (RIPA) requires all material that is intercepted under the authority of a warrant to be handled in accordance with formal arrangements ('safeguards'):

   - section 15 of RIPA requires 'general' safeguards to be in place, to minimise the extent to which material intercepted under warrant is disclosed or copied ('**minimisation** procedures'), and to ensure that the intercepted material is destroyed as soon as its retention is no longer necessary for an authorised purpose ('**destruction** procedures') (**2**);
   - section 16 of RIPA requires 'extra' safeguards to be in place where 'external' warrants are issued in accordance with section 8(4) of RIPA. These govern the selection of material intercepted under the authority of an 'external' RIPA warrant, especially in so far as the targeting of individuals located in the UK is concerned (**3**).

How the Requirements are met

1. This compliance documentation as a whole represents the safeguards formally required by sections 15 and 16 of RIPA as well as by section 4, ISA. They apply to **all** intercepted material, including that intercepted outside the scope of RIPA warrants, and that obtained from collaborating agencies in the UK and abroad. The documentation has been approved on this basis by the Interception of Communications Commissioner, the Intelligence Services Commissioner, and by the Foreign & Commonwealth Office, to the satisfaction of the Secretary of State.

2. Additional requirements, relating to the preservation of records to assist the Investigatory Powers Tribunal, the Intelligence Services Commissioner, and the Interception of Communications Commissioner in the discharge of their duties, is controlled by general guidance on retention and destruction (**⊖ 2**), and in that section of the guidance relating to the Tribunal and Commissioners[1] (**⊖ 4**).

CROSS REFERENCES
⊖ 1 SECTION III: TARGETING AND ANALYSIS
⊖ 2 SAFEGUARDS; 'General' Safeguards required by section 15 of RIPA
⊖ 3 SECTION III: Targeting & Analysis; TARGETING COMMUNICATIONS IN THE UK; THE TARGETING OF EXTERNAL UK COMMUNICATIONS UNDER RIPA
⊖ 4 SECTION VII: Scrutiny of GCHQ activities ("Oversight")

[1] GCHQ policy requires that the reason for the retention of all information must be specifically recorded unless obvious; and, where the records relate to a given individual or organisation, they must be retrievable by reference to that individual or organisation, wherever practicable.

A. MINIMISATION PROCEDURES

General Principles

1. Any information which is disclosed by GCHQ must meet a requirement that is based upon one of the authorised purposes[1]. The extent to which information is disclosed by GCHQ must be limited to the minimum **number of persons** that is relevant to the requirement which the provision of the information is intended to meet[2]. It must also be limited to the minimum **extent** that is necessary to meet the authorised purpose.

2. These obligations apply not just to the original interceptor, but also to anyone to whom the material is subsequently disclosed, whether this is to additional persons within GCHQ or to persons outside GCHQ. Disclosure of information on any subject to organisations beyond GCHQ must be limited to those which have a requirement for it; disclosure by GCHQ must cease if and when the requirement for the information is withdrawn.

[1] **See ⊖ General Principles: GCHQ's Purposes and ⊖ The retention of information for other Authorised Purposes.** If material has been obtained for more than one authorised purpose, its use may be justified on the basis of any **one** of those purposes. Further, information obtained for only one purpose might be retained and used subsequently for a quite different purpose so long as that purpose is also an authorised one.

[2] Some intelligence requirements will entail disclosure to a larger number of recipients than others. In some cases the minimum number of persons might in fact be large, but the principles of minimisation and proportionality apply nonetheless.

Special Considerations required in the reporting of information

The Creation of Records on Individuals And Organisations For Intelligence Purposes

1. Records are part of the essential fabric of intelligence work, enabling requirements to be met through the collation of related information from disparate sources and from differing times.

2. Such records will often contain information about organisations or individuals, which might be characterised as "**personal data**[1]". This is information which relates to an organisation or to a living individual who can readily be identified from that information, or from that plus other information in GCHQ's possession. This has a particular relevance to the ISA and to the HRA because records containing information about an organisation or a living individual provide the best kind of primary indicator that GCHQ has acted in respect of any person who might exercise their right to complain to the Tribunal[2].

3. Consequently, no record can be created or kept by GCHQ, for intelligence purposes, unless it meets an approved **intelligence requirement**, and is needed for the proper discharge of GCHQ's functions (or for other authorised purposes ⇨ 1). The nature of a particular **intelligence requirement** will determine both the need for a record to be established in the first place and the length of time for which it is retained.

---

[1] 'Personal data' is a term of art used in data protection legislation (the *Data Protection Act 1998)*. Certain 'core activity' information has been exempted from the 1998 Act by the Secretary of State on national security grounds. However, records of personal information created or held by GCHQ for 'non-intelligence' purposes, such as records of contractors, or of staff, are included. (See GCHQ Staff Handbook (GSH), Volume 2 - [redacted] Additionally, members of the public have rights of redress before the Investigatory Powers Tribunal for actions taken against them by GCHQ; this includes the creation or retention of GCHQ records (including those exempted as above) in which they are mentioned.

[2] GCHQ is concerned with the activities of individuals acting in a private capacity only to the extent that such activities provide information, which serves a recognised and approved intelligence requirement.

4. To this end, safeguards are in place to ensure that:

   a. all targeting which will lead to the creation of records of personal information receives proper authorisation (⊖ 2);
   b. there is no gratuitous disclosure of personal information (see above);
   c. all retained records containing personal information are distributed and made available only so far as is necessary for the authorised purposes (⊖ 3), and;
   d. all records containing personal information are reviewed periodically and destroyed where appropriate (⊖ 4).

5. These safeguards do not apply to records kept with the subject's actual or implied consent (including any record retained for intelligence purposes which consists solely of publicly available information).

CROSS REFERENCES
⊖ 1 SAFEGUARDS; The Retention of Information for Other Authorised Purposes
⊖ 2 SECTION III: TARGETING AND ANALYSIS
⊖ 3 SAFEGUARDS; 'General' Safeguards required by section 15 of RIPA; MINIMISATION PROCEDURES
⊖ 4 SAFEGUARDS; 'General' Safeguards required by section 15 of RIPA; DESTRUCTION PROCEDURES

Recording and Reporting Confidential Information

1. Analysts will be aware that certain categories of material exist whose inherent nature invokes the need for special handling. Overriding considerations of confidentiality apply to the following categories:

   - **Matters subject to legal privilege.** This is a category of general privilege, with specialised technical rules. The Home Office's guidance on how this privilege relates to interception is reflected here;
   - **Confidential personal information.** This information relates to an individual's physical or mental health, or to their spiritual counselling. It is also a term of art used in Data Processing legislation (➲ 1);
   - **Confidential journalistic information.** Apart from Article 10 ECHR, considerations of good practice attach (➲ 2);
   - **Communications of Members of Parliament.** This is another category of general privilege, extending to all matters connected with proceedings in Parliament; also, the ISA expressly forbids GCHQ from taking any action to further the interests of any United Kingdom political party (➲ 3).

2. RIPA does not provide any special protection for such communications generally, nor for legally privileged communications specifically. But the interception of such communications is, obviously, a particularly sensitive matter, and is subject to the additional safeguards given here. Applications for warrants authorising the direct interception of communications carrying confidential material (as described) will be considered only in compelling circumstances and with full regard to their proportionality.

3. However, such material will usually be acquired by GCHQ consequentially, *i*.e. not by direct targeting, and difficulties arise because the nature of this material may not be readily apparent until **after** the material has been intercepted or processed. The handling and reporting procedures, requiring sensi-checking and limited distributions, should always be heeded. If any interception warrant is likely to give rise to an unusual degree of collateral intrusion involving material of this type, this should be mentioned in the warrant submission so that the Secretary of State can take account of it. The advice concerning indirect targeting should also be heeded (➲ 4).

CROSS REFERENCES
➲ 1 SAFEGUARDS; Safeguards required by The Intelligence Services Act 1994; The Intelligence Services Act 1994 and the Human Rights Act 1998: *The Creation of Records on Individuals And Organisations For Intelligence Purposes*
➲ 2 ZP 307: The Handling of Sensitivities in COMINT
➲ 3 ZP 400: The Communications of Members of the House of Commons and House of Lords
➲ 4 SECTION III: Targeting and Analysis

Legal Professional Privilege

Why Are Lawyers' Communications Special?

1. Although there is no prohibition in UK law to intercepting lawyers' communications, it is an evidential rule in English law that confidential communications for the giving and receiving of legal advice between a lawyer and his client are privileged and cannot be given as evidence in proceedings unless the client waives the privilege. The rule also applies to the production of documents which do not themselves constitute such advice but which are produced for the purposes of litigation. No exceptions are allowed for. (For the purposes of this instruction it should be assumed that this principle of privilege also extends to the legal systems applying elsewhere in the UK).

2. If it were to emerge, in connection with a criminal or civil case, that the Crown had set out to acquire such privileged lawyer-client communications or had not otherwise denied itself the opportunity of reviewing them, there would be very strong grounds for the Court to stop the case on the basis that the Crown had abused its position, and there is a real risk of a breach of the European Convention on Human Rights, in particular Article 6 (right of fair trial).

3. As recognised by Home Office guidelines on this subject, the evidential rule has grown in importance and effect to the point where the Crown takes positive steps to avoid monitoring these communications or to obtain them otherwise.

The Targeting of Lawyers' Communications

4. Persons known to be members of the UK legal profession[1] are not to be targeted unless it is necessary to do so because there are reasonable grounds to believe that they themselves (not their clients[2]) are actively participating in or planning activity which is against the interests of national

[1] This includes any individual, agency or organisation qualified to provide professional legal advice.

[2] Privilege is not lost if a legal adviser is properly advising a person suspected of having committed a criminal offence. However, if the lawyer is aiding and abetting the commission of a future criminal offence by a client (e.g. perverting the course of justice, or evading justice), privilege could be lost.

security, or the economic well-being of the UK, or which in itself constitutes serious crime. Where this is any doubt regarding whether communications are subject to privilege, or whether a legal adviser may be furthering a criminal purpose, advice should be sought from Legal Policy and/or Legal Advisers.

5. Applications for the interception of lawyers should be considered only in exceptional and compelling circumstances with full regard to the proportionality issues that attend such matters. Applications to target members of the UK legal profession must be cleared with Legal Advisers and Legal Policy in addition to any other necessary approvals (such as STA, or RIPA warrants) to ensure that the principles set out above are observed. Any application for a warrant which is likely to acquire communications subject to LPP should include specific statements regarding the necessity for intercepting such a target and how likely it is that privileged communications would be acquired. If one of the express purposes of the warrant is to acquire privileged communications, this should be mentioned also. The Secretary of State may impose additional safeguards on any interception of this type thus authorised.

6. All investigation of lawyers must be notified to the IOC Commissioner and any information derived from such investigations should be made available during the Commissioner's next routine inspection visit.

7. Should it be discovered that a person already being targeted is a member of the UK legal profession, Operational Legalities should be consulted.

Which communications are protected?

8. Communications between a professional legal adviser and his client (or any person representing his client) are privileged[1]:

   - in connection with the giving of legal advice to the client; or
   - in connection with, or in contemplation of, legal proceedings and for the purposes of such proceedings; or
   - between a professional legal adviser or his client or any such representative and any other person in connection with, or in

[1] These definitions are contained in section 78 of the Police Act 1997 and have been adopted by the Home Office for the purpose.

contemplation of, legal proceedings and for the purposes of such proceedings.

9. Legal privilege does not apply to communications made or items held with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or whether he is acting culpably).

The Collection, Reporting and Retention of Lawyers' Communications

10. The more common occurrence would be where lawyers' communications are collected as a consequence of targeting others. Under ZP 307, reporters must submit any intercepted communications involving lawyers and their clients to the [redacted] for sensi-check before it is reported or otherwise disseminated. The [redacted] will consult Operational Policy staff and LA as appropriate.

11. Any dissemination of privileged information should be accompanied by a clear warning that it is subject to legal privilege. Special handling procedures or safeguards should accompany it to ensure that there is no possibility of it becoming available or its content becoming known to the extent that it might prejudice any criminal or civil proceedings related to the information. Where communications involving lawyers are reported, this should be done, whenever possible, without source attribution.

The retention of records subject to LPP

12. Intercepted material that is subject to legal privilege must not be transcribed, retained or copied unless it is necessary for a specified purpose. Any retention or dissemination of privileged information should be accompanied by a clear warning that it is subject to legal privilege. All material thus retained should be notified routinely to the IOC Commissioner during his regular inspection visits, along with any information derived therefrom.

13. If the SDO concludes that intercepted material comprises privileged lawyer client communications that might have a bearing upon proceedings in a UK court or involve the UK legal system, and that the communications do not demonstrate criminal activity by the lawyer, they will be destroyed.

Other categories of Confidential Information

1. The consideration given to communications that are potentially legally privileged should be extended also to communications that involve confidential personal information (including spiritual counselling) and confidential journalistic information. The guidance relating to collateral intrusion should also be heeded and any risks of this happening made clear to the Secretary of State in any warrant application.

Confidential Personal Information

2. Confidential personal information is information held in confidence concerning an individual (whether living or dead), who can be identified from it, and the material in question relates to physical or mental health or to spiritual counselling. This information is held in confidence if it is subject to an express or implied undertaking (including under legislation) or subject to a restriction on disclosure.

Spiritual Counselling

3. This includes contacts between an individual and a Minister of Religion acting as a Minister of Religion. It also includes occasions when an individual is being counselled or seeking the authority of the Divine Being(s) of their faith.

Confidential Journalistic Material

4. This material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it on confidence. It also includes communications resulting in information being acquired for the purposes of journalism and held subject to an undertaking.

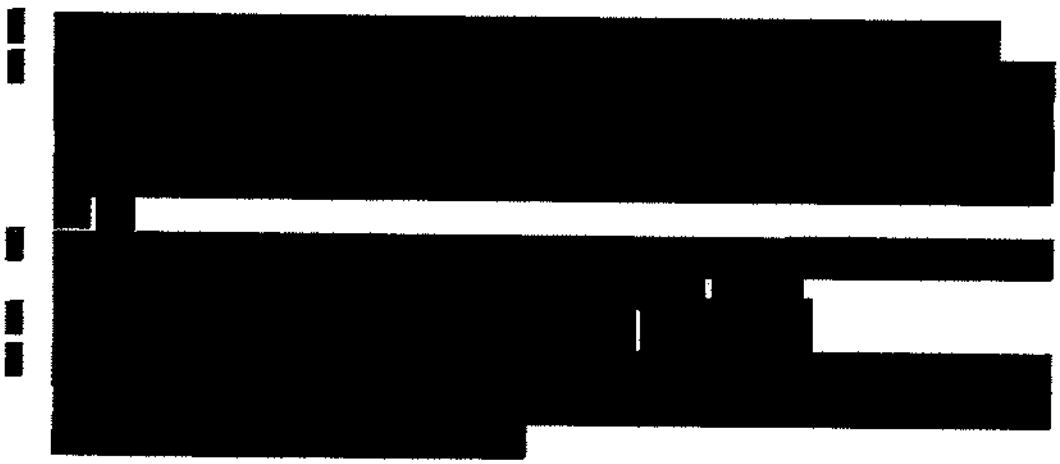
B. DESTRUCTION PROCEDURES

1. Both RIPA and the ISA establish a standard for when intercepted material must be destroyed, but neither attempts to quantify that standard. The nature of a particular intelligence requirement will usually determine the length of time for which intelligence material is kept. The general rule is that intercepted material must be destroyed as soon as it is no longer needed for any of the authorised purposes[1]
(➲ 1)

2. It is the responsibility of the Heads of Business Units (in areas where such records are kept) to ensure that procedures regarding the review and destruction of these records are observed.

Normal Periods for the Retention of Intercepted Material

3. For most categories of intercepted material, the following norms have been agreed. All material should be destroyed as soon as it can be determined reasonably that its retention is no longer necessary, and these time limits should be regarded as *maxima* unless retention beyond that time can be justified, after review, in acceptable terms (see below):



[1] The Tribunal may order the destruction of records if they find against the Department after an investigation: see **SECTION VII: Scrutiny of GCHQ activities ("Oversight")**
[2] This extended retention period is justified by the typical length and complexity of such investigations.

[redacted]

The Retention of Information Beyond the Norms

4. Exceptional examples of retention beyond these norms may be occasioned routinely by areas of GCHQ which specialise in research and development. [redacted]

5. Over and above the requirement to review and retain (or destroy), it is necessary for one archive copy[2] of each end-product report to be retained indefinitely for archive purposes (under the Public Records Act 1958), for intelligence purposes, and for other purposes allowed by the law (➲ 3).

CROSS REFERENCES
➲ 1 General; General Principles; GCHQ's Purposes; SAFEGUARDS; The Release of Information for Other Authorised Purposes
➲ 2 The Retention of Material Obtained for the Purpose of 'preventing or detecting serious crime' ("Serious Crime Material")
➲ 3 General; General Principles; GCHQ's Purposes; SAFEGUARDS; The Release of Information for Other Authorised Purposes

[1] For practical reasons, material of this type is kept on separate databases with limited access.

[2] This might be in hard copy and/or in soft-copy. In both cases, access is strictly limited to those members of staff whose duties make such access necessary, i.e. to those whose duties include the 'other' purposes allowed under the Acts.

The Review of Records

1. All material stored in databases of intercepted material is deleted routinely [redacted] after it is intercepted, whether or not it has been looked at.

2. Any intercepted material which is retained beyond the norms must be reviewed by analysts and reporters at appropriate intervals to confirm that its continued retention is justified. Justification should be in terms of one of the three authorised purposes allowed for by RIPA and by the ISA. Upon review, any records whose retention cannot be justified in these terms should be destroyed.

3. Where any material is retained for longer than the norms specified above, the reason for its continued retention must be recorded in local files, along with the next scheduled review date.

4. Where GCHQ decides to destroy material which it has released to other organisations, those other organisations will be notified automatically of this fact (at least in the case of [redacted] reports, which constitute the majority of such releases). Those organisations then make their own arrangements either to destroy the material as well or to retain and review the material at regular intervals judging by the criteria of necessity.

The Regulation of Investigatory Powers Act 2000: 'Extra' Safeguards Required by section 16 ('external' warrants only)

1. Section 16 of the Regulation of Investigatory Powers Act 2000 provides for safeguards which apply when an 'external' warrant and certificate have been issued in accordance with section 8(4) of the Act.

2. These 'extra' safeguards must:

   a. ensure that intercepted material is *'read, looked at or listened to'* by any person only to the extent that the material is certified; and

   b. regulate the use of selection factors that are referable to individuals known to be for the time being in the British Islands.

3. The guidance given here and in **SECTION III** (on Targeting under an external warrant) constitutes those arrangements which serve the purpose for GCHQ. They have been issued with the approval of the Foreign & Commonwealth Office and are sufficient to allow the Secretary of State to issue 'external' warrants to GCHQ under RIPA.

A. Not '*read, looked at or listened to*' By Any Person

1. The certificate authorises the **examination** of material intercepted under a RIPA 'external' warrant. But this does not give authority to examine indiscriminately (or 'trawl'), since the certificate must specify in advance those intelligence purposes for which the interception of external communications is undertaken; and arrangements must be in place to ensure that material lying outside the ambit of the certificate is not examined. The automated systems which select and process intercepted warranted material lie at the heart of those arrangements for GCHQ (**➲ 1**).

2. Firstly, resource constraints limit the proportion of communications actually intercepted under the 'external' warrant to a small percentage of all those theoretically available[1]; communications not intercepted at this point do not become available to GCHQ, nor can they be retrieved retrospectively.

3. That small proportion of the material actually intercepted is then filtered automatically by selection factors developed by analysts in accordance with the terms of the certificate, and authorised appropriately[2] (**➲ 2**).

4. Only the material which survives this filtering is then available for examination by GCHQ analyst-reporters[3]. The material thus selected is then examined by GCHQ analysts as follows:

- [redacted]

[redacted]

Some processing of the material may be necessary before it can be offered to analysts or reporters in this way.

5. It is possible for material to be selected (and to rest on the database, or be available for listening to) but not be examined before it is deleted.

The Automatic Deletion of Material from the Databases

6. All intercepted material which is stored in databases is deleted a maximum [redacted] after the date of interception, whether it has been examined by that time or not. (Wherever possible, 'deleted' means 'overwritten by other data' but could mean 'rendered inaccessible' if that achieves the purpose). The need to retain the material on the database is reviewed regularly anyway, especially in the case of material obtained for the purpose of preventing or detecting serious crime (➲ 3).

Safeguards Regarding Access To Databases Containing Material Intercepted Under An External Warrant

7. As an extra safeguard, any access to databases which contain material intercepted under a warrant is limited to accredited staff at GCHQ performing a relevant function. All queries entered into the database are authorised in accordance with the procedures laid down in this guidance (➲ 1).

CROSS REFERENCES
➲ 1. 1999 Paper on databases written for the IOCA and ISA Commissioners – Lord Nolan and Stuart-Smith LJ
➲ 2. SECTION III: TARGETING AND ANALYSIS; SECTION IV: SRTD Targeting & Analysis; Definitions

The examination of material that has not been selected for a specific certified purpose

1. Any material that has been intercepted under an 'external' warrant, but not selected in accordance with the certificate, cannot be monitored or examined otherwise, except where the certificate allows it to the extent that it is necessary [1]:

   - to determine whether or not the material falls within the categories of material specified elsewhere in the certificate (➲ 1), or;
   - to maintain an up-to-date knowledge of the communications and technical characteristics of the signals therein (including, but not limited to, how communications are constructed and routed) (➲ 2), or;
   - to maintain or enhance the effectiveness of the interception, selection and subsequent intelligence processes (➲ 2).

2. [redacted]

CROSS REFERENCES
➲ 1. SECTION I: GENERAL; Special Responsibilities for Compliance: The Responsibilities of Dictionary and Directory Managers
➲ 2 SECTION IV: SRTD

[1] Exceptionally, certain categories of material may be fed routinely into a database without selection, where the nature of the intelligence requirement makes initial selection impossible. In these cases, access to the databases is restricted to a very few people and every query made of the database is scrutinised and given appropriate authorisation before being effected.

B. THE TARGETING OF EXTERNAL COMMUNICATIONS UNDER RIPA

1. The procedures adopted to conform with section 16 of RIPA appearing under **SECTION III: Targeting & Analysis; TARGETING COMMUNICATIONS IN THE UK; THE TARGETING OF EXTERNAL UK COMMUNICATIONS UNDER RIPA.**

The Role of the Certificate

2. A warrant which authorises the interception of 'external' communications under RIPA must have associated with it a certificate also authorised by the Secretary of State. The role of the certificate is to regulate the material that can be selected for intelligence purposes.

3. The certificate constitutes one of the main safeguards with relation to external warrants, and any material so intercepted must be selected in terms which relate back to the certificate. There are 3 main categories of selection which are applied to external communications:

   - selection by intelligence topic
   - selection by reference to individuals (known to be for the time being in the UK)
   - selection by reference to individuals (believed not to be in the UK for the time being)

   The guidance, given above in **SECTION III: TARGETING AND ANALYSIS,** should be heeded where 'front-end' selection (usually by dictionary, or TND) is being effected by the use of a selection factor.

4. It is often appropriate to search for previously intercepted material in databases. The same general rules apply to this activity as to 'front end' selection, but analysts must be very careful not to use data-mining procedures where targeting procedures would be more appropriate (➲ 1).

CROSS REFERENCES
➲ 1 TARGETING AND ANALYSIS; Data Mining

Commissioners

A. The Interception of Communications Commissioner

1. Under the Regulation of Investigatory Powers Act 2000 the Prime Minister appoints an Interception of Communications Commissioner (a senior Appeals Court judge) who provides independent oversight of:

    a. the use by the Secretary of State of his/her powers to authorise the interception of communications;

    b. the performance of the duties imposed on the Secretary of State by the interception provisions of RIPA;

    c. the use by senior officers in GCHQ of their powers to authorise the continued interception of communications belonging to an individual located in the UK, under section 16(5) RIPA;

    d. the use by relevant authorities of their powers to authorise the obtaining of communications data, and their performance of the duties imposed on them;

    e. the adequacy of the safeguards required under sections 15 and 16 of the Act (⊖ 1);

    f. the use by relevant authorities of their powers regarding encryption (once Part III RIPA comes into force).

B. The Intelligence Services Commissioner

2. Under the Regulation of Investigatory Powers Act 2000, the Prime Minister also appoints an Intelligence Services Commissioner (also a senior Appeals Court judge) who provides independent oversight of the exercise by the Secretary of State of his powers under sections 5 to 7 of the Intelligence Services Act 1994 (warrants for interference with wireless telegraphy, entry and interference with property, authorisations under section 7, *etc.*)[1]

[1] See ⊖ Investigatory Powers Tribunal and ⊖ ISA Warrants.

[redacted]

Auditing GCHQ's Targeting

The purpose behind audit

1. In order to justify any interference with rights that are guaranteed under the ECHR (such as the right to privacy given in Article 8), a public authority must be able to demonstrate that the interference:

   - **is prescribed by the law**
   - GCHQ operations must comply with the Regulation of Investigatory Powers Act 2000 and the ISA 1994;
   - **has an aim which is legitimate under Article 8, paragraph 2**
   - GCHQ's operations must have, as their legitimate aim, one or more of the authorised purposes which appear in Article 8, paragraph 2: a JIC priority or purpose (NS, EWB, SC); and a MIRANDA number;
   - **is necessary in a democratic society**
   - the necessary interference must be convincingly established and proportionate to the 'legitimate aim' being pursued;
   - the reasons given (in the justification field) must be both relevant and sufficient

2. The proportionality test ensures that the legitimate aim is pursued with the minimum impairment of an individual's rights established under Article 8. The test requires a public authority to adopt the least drastic method of achieving the aim, but it should not restrict the authority unduly in what it is trying to achieve legitimately.

How the purposes are to be achieved

3. The following questions need to be addressed by those conducting the audit:

   (Q1) Does this targeting require a RIPA warrant? Has one been obtained? If so, does this targeting relate sensibly to its terms?

[redacted]

(Q3) For all targeting:

- Is there a valid [redacted] number and JIC priority that relates sensibly to the targeting?
- Is the justification convincingly established in relevant and sufficient terms? (Does it say *'development - suspected from call records of being associated with established SC target x'* or does it say simply *'associated with x'*?)
- What kind of output would the targeting produce? Is the targeting framed in terms that can be considered proportionate?
- Do any of the [redacted] fields need to be updated?
- Should the productivity of this targeting be reviewed?

The Auditing Procedure

4. The audit should aim to embrace a representative sample of a section's targeting; this will vary from section to section, with a quality control role assigned to the IPT Head (see below).

5. The steps to be undertaken are as follows:

   (a) All numbers targeted that have not hit over the previous 6 months will be deleted before audit unless the 'owner' analyst can justify their continued targeting. These numbers will be included with the final 'numbers audited' figure.

   (b) [redacted] will be interrogated to provide a maximum of 100 numbers per production team. This should produce the basis for a random but representative sample.

   (c) A selection of targeted numbers will be output, along with other relevant [redacted] fields, in a worksheet format. This worksheet (suitably annotated) will serve as the initial output from the audit.

   (d) One representative per team will be nominated to be responsible for each audit; the representatives will change from audit to audit. The representatives in each IPT would get together and co-ordinate a selection from their list(s) a 'set' that would be representative of the section's activity as a whole. Each representative will then 'swap' their list with another representative within the IPT, who will conduct the

audit of those numbers according to the published standards (see above), consulting with the originator of the targeting as necessary.

(e) The worksheets will be given to the IPT Head for collation.

6. It is expected that this routine will be followed at least once every 3 months, but the decision on frequency should be left to IPT Heads.

Auditing the Output

7. The IPT Head plays the key role in establishing acceptable standards for the section to attain and in deciding exactly how frequently the audits should be held. An independent voice (preferably another IPT Head) should be introduced at the stage when the audits are being assessed, and conclusions drawn. (This should also help to develop consistent standards across IPTs).

8. IPT Heads should produce a formal audit report at least once a year. The reports should indicate the extent of the audit actually carried out; any special factors that may have influenced the methodology chosen for the audit; what the audits have revealed and how problems will be remedied. There should be a declaration from the IPT Head that, to the best of his/her knowledge and ability, the audit has attained the standard(s) set in this guidance.

9. It is implicit in this arrangement that the IPT Head must pay special attention to the amount of targeted numbers actually covered by the audits, and to the % rate of corrections that are required to bring the system up to standard. An high 'error:numbers_audited' rate would require the IPT Head to impose a higher standard of audit the next time around (most obviously, by increasing the numbers audited). This would be in accordance with standard auditing procedures.

10. Every year, IPT Heads will collate the output from audit and make a declaration of compliance to the [redacted]

COMMUNICATIONS DATA

1. 'Communications data' refers to the data exchanged between telecommunications providers that relate to 'call events'[1]. It includes the calling and called addresses, whether the attempt to call was successful, and the time and duration of the call. It does not include any of the contents of the call or, say, any interaction with a website[2]. The provisions contained in RIPA Part I Chapter II (sections 21 to 25) provide a (non-exclusive) *regime* for the acquisition and disclosure of communications data. The Interception of Communications Commissioner has oversight of all Notices and Authorisation issued under Part I Chapter II RIPA – see **SECTION VII OVERSIGHT.**

Definition of communications data

2. Under RIPA, communications data are defined as:

   (a) any traffic data[3] comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any telecommunication system by means of which it is being or may be transmitted[4];

   (b) any information which includes none of the contents of a communication and is about the use made by any person of a telecommunications service; or is in connection with the provision to or use by any person of any telecommunications service[5];

   (c) any other information that is held or obtained, in relation to persons to whom he provides the service, by a person providing a telecommunications service[6].

---

[1] 'Call' is used here to denote not only telephone calls but also data network communications, *e.g.* email, or facsimile, etc.
[2] 'Communications data' includes internet addresses to the extent that they identify a network or host computer. It does not include page content hosted on that site.
[3] "traffic data", in relation to any communication, means (a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted, (b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted, (c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and (d) any data identifying the data or other data as data comprised in or attached to a particular communication.
[4] CLI and DNR information is regarded as falling within this category.
[5] Itemised billing, whether call minder or call forwarding facilities are used falls within this category.
[6] Historical data such as credit card details of bill payee, or the email address owner would fall within this category.

[redacted]

3. Communications data do not constitute a "communication" under the terms of RIPA, so RIPA safeguards do not apply to them, unless they have been obtained pursuant to a RIPA warrant (see below). The point is moot, however, since the safeguards contained in the Compliance Documentation apply equally to all material acquired by GCHQ.

GCHQ's sources of communications data

1. GCHQ finds it necessary to obtain communications data both to produce intelligence in its own right (*e.g.* by building up a network chart of a suspected criminal's associates), and to steer interception operations authorised under RIPA (*e.g.* by indicating which of the available communications need to be intercepted in order to provide the material required for intelligence purposes). This material is then retained in GCHQ databases that may be accessed by staff – see section about '**Accessing communications data**' below.

2. GCHQ typically requests the following categories of communications data from CSPs:

   a. **subscriber-related information**, such as subscriber details for a given telecommunications address, lists of telecommunications addresses associated with a given premises, reverse name searches, tip-offs if telecommunications addresses reassigned to different subscribers, tip-offs if subscriber ports telecommunications address to a different CSP, etc;

   b. **billing information**, such as requests for billing on specific telecommunications addresses and details of when a subscriber was last active;

   c. **target-specific research**, such as feasibility checks prior to warrant signature or implementation, [redacted]

   d. **call diverts or collation of calls** to a number of interest.

3. These communications data are obtained by GCHQ under the following legal authorisations.

A. 'external' warrants under RIPA

4. Where GCHQ is authorised under a RIPA warrant to intercept communications, the acquisition of related communications data is also authorised[1]. GCHQ also

[1] See section 5(6): '*The conduct authorised by an interception warrant shall be taken to include- [...] (b) conduct for obtaining related communications data*', where "related communications data", means such communications data as '*(a) is obtained by, or in connection with, the interception; and (b) relates to the communication or to the sender or recipient, or intended recipient, of the communication*': section 20, RIPA.

creates communications data from intercepted communications. RIPA safeguards apply to such communications data (but see above).

5. CSPs may also provide communications data on a voluntary basis[1].

B. The Telecommunications Act 1984: a section 94 direction

6. Under section 94(1) of the Telecommunications Act 1984, the Secretary of State may give a communications service provider a direction in terms that are *'requisite or expedient in the interests of national security'* (or for other reasons not relevant here). There must have been previous consultation with the provider.

7. The scope of the request is marked out by the terms of the directive itself, and may be on a continuing basis. Communications data may be acquired by GCHQ on this basis. Provided that the whole direction is expedient for the national security purpose, there is no legal bar to GCHQ using the data thus acquired for other lawful purposes.

C. Part I Chapter II RIPA

8. Part I, Chapter II of RIPA allows GCHQ staff to supplement the communications data acquired under A. or B. above to meet the necessary requirements of their work. It allows 'designated persons' within an organisation to authorise certain conduct:

   a. An **authorisation** allows a public authority to collect or to retrieve the communications data itself[2] (*section 22(3)*), and;
   b. A **notice** is given to the Communications Service provider (CSP) and allows that operator to collect or retrieve the data[3] and to provide the material to the public authority that served the notice (*section 22(4)*).

[1] Voluntary provision by the CSPs raises Data Protection and customer confidentiality issues for the CSP, for which they will probably require assurance.
[2] An authorisation would apply where there is a prior agreement in place between a public authority and the CSP regarding methods or mechanisms for disclosure, or where the CSP is not capable of fulfilling the request.
[3] *i.e.* the notice may authorise the CSP to collect data not yet acquired as well as authorising them to disclose material already acquired.

Acquisition Process for communications data under RIPA Part I Chapter II

1. A GCHQ analyst, while pursuing an authorised intelligence requirement, may identify a need to acquire communications data for a UK telephone number, or for an entity who is known to be in the UK at the time of the request.

2. The analyst will need to consider whether an authorisation or notice under RIPA Part I, Chapter II is required[1]. As a general rule, the RIPA provisions should be used by GCHQ staff to acquire the following categories of communications data:

   - subscriber information for all UK[2] numbers;
   - billing data and feasibility checks for all UK telephone numbers, and;
   - geo-location where the user is known to be located in the UK.

3. [redacted]

[1] The application forms will allow for either form of request, so a positive choice must be made.
[2] The acquisition of communications data for overseas telephone numbers is fully covered by the external warrants that the Secretary of State has signed for GCHQ (see above), so no further authorisation is needed.

4. In such cases, the analyst must complete one of the approved application forms provided in order to effect the request[1]. Requests for these data will not be effected otherwise within GCHQ. All conduct thereby authorised must be carried out in accordance with the terms of that authority.

The criteria to be satisfied

5. In making an application to acquire communications data under Part I, Chapter II RIPA, the form must describe fully and exactly:

   - The name and/or designator of the officer making the request, and;
   - The operation or person to which the communications data relates, and;
   - A description of the information being requested, and;
   - the authorised purpose for which this information is **necessary** (in the interests of national security, or the economic well-being of the UK, or for the prevention or detection of serious crime[2]), and;
   - the **proportionality** of the request (how the acquisition of communications data is a reasonable method of achieving the authorised purpose[3]), and;
   - any urgent timescale within which the communications data is required.

6. Each application should have a unique reference identifying it

7. A reference to any extant RIPA warrant or STA against the same target should be enough to satisfy the justification and proportionality requirements, because those considerations would have been taken into account already.

[1] [redacted]

[2] These purposes are all included in section 22(2) of the Act, along with other purposes outside the statutory remit of GCHQ. Where the economic well-being purpose is specified, it must be related directly to national security and the direct link must be explained fully in the application.

[3] The conduct must not be excessive, arbitrary or unfair: see the general guidance on proportionality.

Who is authorised to sign?

8. The application form must be approved by a '**designated officer**'. [redacted] are 'designated officers' for the purpose of authorising the acquisition of communications data or for the serving of a notice.

9. The designated officer must:

   (a) ensure that the tests of necessity and proportionality are met in each application, *viz.*

   - That the case justifies the necessity of accessing and obtaining communications data for an authorised purpose[1];
   - That obtaining access to the data by the conduct authorised is proportionate to what is sought to be achieved[2];
   - That the circumstances of the case justify the access if there is a risk of collateral intrusion,

   and;

   (b) Whether any urgent timescale is justified, and;
   (c) ensure that the forms are otherwise completed fully and accurately, and;
   (d) decide whether or not authorisation should be granted or the notice given[3], and
   (e) sign and date the form.

10. Multiple numbers may be entered on to a form where they are linked by the same intelligence case, the same justification, the same level of intrusion, and where the proportionality argument applies equally to all.

[1] Where feasibility checks are being requested, it will be enough to refer to the warrant application being made (with details allowing that case to be retrieved).
[2] The designated officer must be careful to scrutinise every number on the application form. Where subscriber details are being requested to be included in a call records chart, the proportionality argument is likely to alter according to the degree of separation of the number from the main target(s) – separate forms may be needed for each degree of separation or inference.
[3] The Single Point(s) of Contact (SPOCs) will be able to advise.

Single points of contact (SPOCs)

11. SPOCs must exist within each public authority which intends to apply for communications data in order to:

    a. assess whether the CSP can reasonably provide access to the wanted communications data, and;
    b. advise on the practicalities of accessing different types of communications data from different CSPs, and;
    c. provide CSPs with safeguards for authentication, and;
    d. in liaison with others within the Department, to assess any cost and resource implications both to the Department and to the CSP.

12. All notices and authorisations must be channelled through the SPOCs. SPOCs may also be the persons to whom CSPs initially disclose (if not the designated person).

13. The identities of these individuals within GCHQ will be agreed with the CSPs and recorded; the lists will need to be available to those that need to know.

Expiry, cancellation and renewal of authorisations and notices

1. Authorisations and notices are valid for a maximum period of one month (starting from the date on which the authorisation is granted or the notice given). A shorter period of time may be specified if appropriate. Where the request is for "historical" data, the request will relate only to material already acquired by, or in the possession of, the CSP. Where the request anticipates the continuing disclosure of "future" communications data, disclosure may only be required of data obtained by the CSP within this period *i.e.* up to one month.

2. The CSP must comply with a notice as soon as is reasonably practicable (but may not comply if that is not reasonably practicable).

3. An authorisation or notice may be renewed at any time during the month that it is valid. The same procedure must be followed as in obtaining a fresh authorisation or notice. A renewed authorisation or notice takes effect at the point at which the one that it is renewing expires.

4. The designated person must cancel a notice as soon as it is no longer necessary, or as soon as the conduct can no longer be considered proportionate. The duty to cancel a notice falls on the designated person who issued it, although any designated officer may issue the cancellation if the original designated officer is not available. The relevant CSP must be informed of the cancellation as soon as is reasonably practicable.

5. Where the disclosure of communications data is required urgently, consult operational legalities.

The Retention of records for oversight purposes

1. As stated above, the Interception of Communications Commissioner has oversight of all Notices and Authorisation issued under Part I Chapter II RIPA. For this reason, copies of each application form and each authorisation granted or notice issued must be retained for potential examination by the Commissioner, or by his staff. The records must also make it clear when the authorisation or notice started and when it ended (or was cancelled). Both the analyst who applied for the communications data and the designated officer who authorised it may be required to explain their decisions to the Commissioner or to his staff.

2. The application forms (whether approved by the designated officer or not) must be retained by the relevant Production Unit for this purpose. Applications, authorisations and notices for communications data must be retained by GCHQ at least until they have been audited by the Commissioner and for long enough to allow the Investigatory Powers Tribunal to carry out its functions. (Currently, a [redacted] – see SECTION VIII – HANDLING OF COMPLAINTS). It must be possible to refer to each completed authorisation or notice by a unique reference number and for all product that follows from the communications data having been acquired to be identified.

3. Where any errors have occurred (*i.e.* where data have been acquired without the necessary authority or where authorities have been sanctioned incorrectly) a record should be kept and a report and explanation sent to the Commissioner as soon as practical. In the first instance, the person who discovers the error should contact Operational Legalities, who will involve legal advisers as necessary.

Accessing communications data held on GCHQ databases

4. GCHQ stores communications data it has acquired in a variety of databases.

5. Because the acquisition of the material thus stored has been justified already (through GCHQ's existing interception warrants or the section 94 direction), and the acquisition of communications data is not as intrinsically intrusive as interception, no additional justification is needed simply to access these data whether or not a UK number is involved. The subsequent use of these data is proportionate in HRA terms, assuming that the use to which the data is put is within the purposes set out in section 4(2) ISA, *i.e.* national security, serious crime or the economic well being of the UK.

6. However, to provide the necessary level of assurance so that GCHQ is able properly to answer complaints to the IP Tribunal (and in so doing provide evidence that we are acting proportionately), any [redacted] derived from such material which has been accessed is also searched in response to any complain received from the IP Tribunal.

THIS PAGE IS LEFT BLANK INTENTIONALLY