APPENDIX

THE EQUIPMENT INTERFERENCE REGIME

1. The Equipment Interference Regime which is relevant to the activities of GCHQ principally derives from the following statutes:

   (a) the Intelligence Services Act 1994 ("**the ISA**"), (as read with the Counter-Terrorism Act 2008 ("**the CTA**") and the Computer Misuse Act 1990 ("**the CMA**"));

   (b) the Human Rights Act 1998 ("**the HRA**");

   (c) the Data Protection Act 1998 ("**the DPA**"); and

   (d) the Official Secrets Act 1989 ("**the OSA**").

2. In addition, the draft Equipment Interference Code of Practice dated February 2015 ('**the EI Code**') and the Covert Surveillance and Property Interference Code of Practice 2002 ('**the Property Code'**)[1] are relevant to the regime as regards the scope of any powers to interfere with property and equipment.

3. There are also important **oversight mechanisms** in the regime provided by the Intelligence Services Commissioner, the Intelligence and Security Committee and the Tribunal.

4. In addition and in accordance with the Codes, GCHQ has a number of **internal arrangements** in relation to CNE activities; an open summary of which appears at the end of this Appendix.

The ISA (read with the CTA and the CMA)

GCHQ functions

5. By s. 3(1)(a) of the ISA, the functions of GCHQ include the following:

   "... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material ...."

6. By s. 3(2) of the ISA, these functions are only exercisable:

   "*(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*
   (b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or
   (c) in support of the prevention or detection of serious crime."

7. GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

   "... that there are arrangements for securing that no information is obtained by GCHQ

[1] The Property Code was first issued in 2002 and further versions of the Code were published in 2010 and on 10 December 2014 (in terms of property interference there is no material difference between the 2010 and the 2014 versions of the Code).

except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ..."

Disclosure of information

8. By s. 19(5) of the CTA, information obtained by GCHQ for the purposes of any of its functions "*may be disclosed by it - (a) for the purpose of the proper discharge of its functions, or (b) for the purpose of any criminal proceedings*."

9. Thus, specific statutory limits are imposed on the information that GCHQ can obtain, and on the information that it can disclose. In addition, the term "information" is a very broad one, and is capable of covering *e.g.* both communications and communications data.

10. By s. 19(2) of the CTA:

"*Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions*."

Computer Misuse Act ('CMA')

11. The Computer Misuse Act 1990 (CMA) came into force on 29 June 1990. It was amended on 3 May 2015 as a result of changes introduced by the Serious Crime Act 2015.

12. By s.1(1) of the CMA:

"*(1) A person is guilty of an offence if—*
(a) he causes a computer to perform any function with intent to secure access to any program or data[2] *held in any computer;*

---

[2] Section 17 of the CMA provides, *inter alia*, that:

(2) A person ***secures access to any program or data*** *held in a computer if by causing a computer to perform any function he –*

(a) alters or erases the program or data;
(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
(c) uses it; or
(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);

and references to access to a program or data (and to an intent to secure such access [or to enable such access to be secured] 1) shall be read accordingly.

(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform –

(a) causes the program to be executed; or
(b) is itself a function of the program.

(4) For the purposes of subsection (2)(d) above –

(a) a program is output if the instructions of which it consists are output; and
(b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial. ...

(6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(b) the access he intends to secure, is unauthorised[3]*; and*
(c) he knows at the time when he causes the computer to perform the function that that is the case."

13. Although "*computer*" is not defined in the CMA, in the context of s.69 of the Police and Criminal Evidence Act 1984 (PACE), the term has been held to mean "*a device for storing, processing and retrieving information*" (see *DPP v McKeown* [1997] 1 WLR 295 at 302).

14. By s.3 of the CMA it is also an offence to do any unauthorised act[4] in relation to a computer, if, at the time that he does the act the person knows that it is unauthorised (s. 3(1)) and either (1) the intention is to impair the operation of any computer; to prevent or hinder access to any program or data held in any computer; to impair the operation of any such program or the reliability of any such data (s. 3(2)(a)-(c)), or (2) the person is reckless as to whether the act will do any of those things s. 3(3)).

15. Section 4 of the CMA sets out the territorial scope of, *inter alia*, offences under s. 1 and s. 3 of the CMA. In particular this makes clear that it is immaterial for the purposes of any offence under s.1 or s.3 of the CMA (a) whether any act or other event, proof of which is required for conviction of the offence, occurred in England or Wales; or (b) whether the accused was in England or Wales at the time of any such act or event. Save in respect of certain offences (i.e. under s. 2 of the CMA), at least one significant link with domestic jurisdiction must exist in the circumstances of the case for an offence to be committed. The tests as to whether there is a significant link with domestic jurisdiction are set out in section 5 of the CMA.

16. Summary conviction under the CMA in respect of offences under s. 1 and s. 3 may lead to imprisonment for a term not exceeding 12 months or a fine (see s. 1(3)(a) and s. 3(6)(a) CMA). Any conviction on indictment may lead to imprisonment for a term not exceeding 2 years or to a fine, or both, in respect of a s. 1 offence (see s. 1(3)(c)) and for a term not exceeding 10 years, or to a fine, or both in respect of a s. 3 offence (see s. 3(6)(c) CMA).

17. Section 10 of the CMA (prior to amendments introduced on 3 May 2015) provided as follows:

> "*Saving for certain law enforcement powers*
> *Section 1(1) above has effect without prejudice to the operation –*
> *(a) In England and Wales of any enactment relating to powers of inspection, search or seizure*."

18. On 3 May 2015 the CMA was amended. Those amendments (which it is accepted are not retrospective) included, *inter alia*:

a) Changes to the test under section 5 as to when a significant link with domestic

---

[3] By section 17(5) of the CMA – "*Access of any kind by any person to any program or data held in a computer is unauthorised if— (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled"* (NB. this subsection is subject to section 10 which contains a saving in respect of certain law enforcement powers).

[4] By s. 17(8) of the CMA - *An act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done)– (a) is not himself a person who has responsibility for the computer and is entitled to determine whether the act may be done; and (b) does not have consent to the act from any such person. In this subsection "act" includes a series of acts.*

jurisdiction is established in respect of offences under, *inter alia*, sections 1 and 3 of the CMA;

b) Changes to section 10 of the CMA, which now provides *inter alia*:

> "*Savings*
> *Sections 1 to 3A have effect without prejudice to the operation—*
> *(a) in England and Wales of any enactment relating to powers of inspection, search or seizure or of any other enactment by virtue of which the conduct in question is authorised or required...*" (changes underlined)

Authorisation for equipment interference

s.5. warrants

19. By s. 5 of the ISA the Intelligence Services, including GCHQ, can apply for a warrant which provides specific legal authorisation for property interferences by them. Thus by s5(1) of the ISA:

> *"(1) No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section.*

20. In relation to GCHQ, pursuant to s.5(2)(a)-(c) of the ISA the Secretary of State can only issue a warrant under s.5 following an application by GCHQ if he/she is satisfied that:

> (a) it is **necessary** for the action to be taken for the purpose of assisting GCHQ in carrying out its statutory functions under s. 3(1)(a) of the ISA;
> (b) the taking of the action is **proportionate** to what the action seeks to achieve; and
> (c) **satisfactory arrangements** are in force under section 4(2)(a) of the ISA with respect to the disclosure of information by GCHQ obtained by virtue of the section and any information obtained under the warrant will be subject to those arrangements.

21. When exercising his/her discretion and considering necessity and proportionality, the Secretary of State must take into account "*whether what it is thought necessary to achieve by the conduct authorised by the warrant could reasonably be achieved by other means*" (s.5(2A) ISA).

22. Pursuant to s. 5(3) of the ISA GCHQ may not be granted a s.5 warrant for action in support of the prevention or detection of serious crime which relates to property in the British Islands.

23. By s.6 of the ISA the procedure for issuing warrants and the duration of s. 5 warrants is addressed. In particular s.6(1) provides that a warrant shall not be issued save under the hand of the Secretary of State, unless it is a species of urgent case as set out in s.6(1)(b) or (d)[5].

24. In terms of duration, unless the warrant is renewed, it ceases to have effect at the end of the period of six months, beginning with the day on which it was issued (s. 6(2)) (save where the warrant was issued urgently and not under the hand of the Secretary of State in which case it

[5] Those sub-sections provide:
(b) in an urgent case where the Secretary of State has expressly authorised its issue and a statement of that fact is endorsed on it, under the hand of a senior official; ...
(d) in an urgent case where the Secretary of State has expressly authorised the issue of warrants in accordance with this paragraph by specified senior officials and a statement of that fact is endorsed on the warrant, under the hand of any of the specified officials.

lasts for 5 working days).

25. As to renewal, under s.6(3) of the ISA, if, before the expiry of the warrant, the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, it may be renewed for a period of six months.

26. By s. 6(4) of the ISA "*The Secretary of State shall cancel a warrant if he is satisfied that the action authorised by it is no longer necessary".*

s.7 authorisations

27. In terms only of acts outside the British Islands, s.7 of the ISA also provides for the authorisation of such acts by the Intelligence Services including GCHQ. S.7(1) and 7(2) provide:

"*(1) If, apart from this section; a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section.*

(2) In subsection (1) above "liable in the United Kingdom" means liable under the criminal or civil law of any part of the United Kingdom."

28. Acts outside the British Islands include cases where the act is done in the British Islands, but is intended to be done in relation to apparatus that is or is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus (s. 7(9) ISA).[6]

29. However, pursuant to s.7(3) of the ISA, the Secretary of State shall not give an authorisation under s. 7 of the ISA to GCHQ unless he/she is satisfied:

"(a) that any acts which may be done in reliance on the authorisation or, as the case may be, the operation in the course of which the acts may be done will be necessary for the proper discharge of a function of GCHQ; and

(b) that there are satisfactory arrangements in force to secure—

> *(i) that nothing will be done in reliance on the authorisation beyond what is necessary for the proper discharge of a function of ...GCHQ; and*
>
> *(ii) that, in so far as any acts may be done in reliance on the authorisation, their nature and likely consequences will be reasonable, having regard to the purposes for which they are carried out; and*

(c) that there are satisfactory arrangements in force under section... 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained by virtue of anything done in reliance on the authorisation will be subject to those arrangements.

30. Under s. 7(4) of the ISA such an authorisation by the Secretary of State:

---

[6] In addition ss.7(10)-(14) of the ISA recognise that it may be difficult, in certain circumstances to ascertain reliably the location of property and therefore provide, *inter alia*, that where acts are done in relation to property which is eg. mistakenly believed to be outside the British Islands, but which is done before the end of the 5th working day on which the presence of the property in the British Isles first becomes known, those acts will be treated as done outside the British Islands.

"*(a) may relate to a particular act or acts, to acts of a description specified in the authorisation or to acts undertaken in the course of an operation so specified;*

(b) may be limited to a particular person or persons of a description so specified; and

(c) may be subject to conditions so specified."

31. Consequently the type of acts which may be covered by a s. 7 authorisation are broadly defined in the ISA and can clearly cover equipment interference outside the British Islands, where the tests in s. 7(3) of the ISA are satisfied.

32. By s. 7(5) of the ISA, an authorisation shall not be given except under the hand of the Secretary of State, or in an urgent case and where the Secretary of State has expressly authorised it to be given under the hand of a senior official.

33. In terms of duration, unless it is renewed, a s. 7 authorisation ceases to have effect at the end of the period of six months beginning on the day on which it was given (save if it was not given under the hand of the Secretary of State in which case it lasts for 5 working days) (see s. 7(6) ISA).

34. Pursuant to s. 7(7) the authorisation can be renewed for a period of six months, if the Secretary of State considers it necessary to continue to have effect for the purpose for which it was given.

35. By s. 7(8) of the ISA "*The Secretary of State shall cancel an authorisation if he is satisfied that the action authorised by it is no longer necessary".*

36. Consequently both s. 5 warrants and s.7 authorisations provide the Intelligence Services, including GCHQ, with specific legal authorisation for equipment interference, with the effect that the Intelligence Services are not civilly or criminally liable for such interferences, including under the CMA.

The Equipment Interference Code of Practice ('the EI Code')

37. The draft Equipment Interference Code of Practice ('the EI Code') was published on 6 February 2015 by the Home Office. It was issued pursuant to section 71 of RIPA[7] and was subject to public consultation between 6 February 2015 and 20 March 2015 in accordance with s. 71(3) of RIPA. On 4 November 2015 an amended version of the Code was laid before both Houses of Parliament and must now be the subject to affirmative resolution by both Houses (see draft 'The Equipment Interference (Code of Practice) Order 2015').

38. However, as set out in the Written Ministerial Statement which accompanied the publication of the draft Code in February 2015, the safeguards in that Code reflected the safeguards

[7] S. 71 of RIPA imposes a duty on the Secretary of State to issue, following appropriate consultation, one or more codes of practice relating to the exercise and performance of the powers and duties conferred or imposed by or under, *inter alia*, section 5 of the 1Intelligence Services Act 1994. Any person exercising or performing any power or duty in relation to which provision may be made by a code of practice under section 71, must have regard to any relevant provisions of every code of practice for the time being in force: s. 72(1). Further, where the provision of a code of practice appears to the Tribunal, a court or any other tribunal to be relevant to any question arising in the proceedings, in relation to a time when it was in force, that provision of the code must be taken account in determining that question. A similar duty is imposed on the Commissioner: see s. 72(4) of RIPA. The code of practice can be taken into account in assessing "foreseeability" for the purposes of Art. 8(2): *Kennedy v United Kingdom* (2011) 52 EHRR 4, at §157.

applied by the relevant Agencies, including GCHQ. GCHQ can confirm that it complies with all aspects of the EI Code and can also confirm that it fully reflects the practices, procedures and safeguards which GCHQ has always applied to any equipment interference activities carried out by it.

39. As to the differences between the draft Code dated 6 February 2015 and the Code as recently laid before Parliament in November 2015, the two changes of substance are as follows:

(a) In Chapter 3 dealing with Legally Privileged and Confidential Information there are some changes to §§3.4 to 3.14 including, *inter alia*, new text in 3.4 and 3.11-3.12 and changes in 3.6-3.10 as compared with 3.5-3.8 of the draft Code. There is also a change to the last sentence of §3.25 and 3.28 is new text.

(b) In Chapter 5 dealing with record keeping, three new bullets have been added (bullets 1, 3 and 4) as they appear at §5.1 so that there are more detailed requirements for record-keeping.

40. Otherwise there have been minor tweaks to the language of the Code, for example, in §§1.7, 6.5, 6.11, 7.1, 7.2, 7.12, 7.13, 7.14 and 7.6 the word "should" now appears instead of the word "must".

41. The EI Code provides guidance on the use by the Intelligence Services of s. 5 and s.7 of the ISA to authorise equipment interference to which those sections apply. In particular it provides guidance on the procedures that must be followed before equipment interference can take place, and on the processing, retention, destruction and disclosure of any information obtained by means of the interference.

42. To the extent that the EI Code overlaps with the guidance provided in the Covert Surveillance and Property Interference Revised Code of Practice issued in 2014 (see further below), the EI Code takes precedence, however the Intelligence Services must continue to comply with the 2014 Code in all other respects (see §1.2).

43. The EI Code also records the fact that there is a duty on the heads of the Intelligence Services to ensure that *arrangements* are in force to secure: (i) that no information is obtained by the Intelligence Services except so far as necessary for the proper discharge of their statutory functions; and (ii) that no information is disclosed except so far as is necessary for those functions (see §1.3 of the EI Code and the statutory framework under the ISA set out above).

Equipment interference to which the EI Code applies

44. The EI Code identifies specific types of equipment interference to which the code applies. At §1.6 it states:

"*This code applies to (i) any interference (whether remotely or otherwise) by the Intelligence Services, or persons acting on their behalf or in their support, with equipment producing electromagnetic, acoustic and other emissions, and (ii) information derived from any such interference, which is to be authorised under section 5 of the 1994 Act, in order to do any or all of the following:*

a) obtain information from the equipment in pursuit of intelligence requirements;
b) obtain information concerning the ownership, nature and use of the equipment in pursuit of intelligence requirements;
c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);
d) enable and facilitate surveillance activity by means of the equipment.

"Information" may include communications content, and communications data as defined in section 21 of the 2000 Act."

45. At §1.7 of the EI Code it summarises the effect of a s.5 warrant and states:

"*The section 5 warrant process must [should[8]] be complied with in order properly and effectively to deal with any risk of civil or criminal liability arising from the interferences with equipment specified at sub-paragraphs (a) to (d) of paragraph 1.6 above. A section 5 warrant provides the Intelligence Services with specific legal authorisation removing criminal and civil liability arising from any such interferences.*"

Basis for lawful equipment interference activity

46. In addition to highlighting the statutory functions of each Intelligence Agency, the EI Code specifically draws attention to the HRA and the need to act proportionately so that equipment interference is compatible with ECHR rights. At §§1.10-1.13 the EI Code states:

"*1.10 The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, such as the prohibition on torture, while others are qualified, which means that it is permissible for public authorities to interfere with those rights if certain conditions are satisfied.*

1.11 Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when the Intelligence Services seek to obtain personal information about a person by means of equipment interference. Such conduct may also engage Article 1 of the First Protocol (right to peaceful enjoyment of possessions).

1.12 By section 6(1) of the 1998 Act, it is unlawful for a public authority to act in a way which is incompatible with a Convention right. Each of the Intelligence Services is a public authority for this purpose. When undertaking any activity that interferes with ECHR rights, the Intelligence Services must therefore (among other things) act proportionately. Section 5 of the 1994 Act provides a statutory framework under which equipment interference can be authorised and conducted compatibly with ECHR rights.

1.13 So far as any information obtained by means of an equipment interference warrant is concerned, the heads of each of the Intelligence Services must also ensure that there are satisfactory arrangements in force under the 1994 Act or the 1989 Act in respect of the disclosure of that information, and that any information obtained under the warrant will be subject to those arrangements. Compliance with these arrangements will ensure that the Intelligence Services remain within the law and properly discharge their functions."

General rules on warrants

47. Chapter 2 of the EI Code contains a number of general rules on warrants issued under s. 5 of the ISA.

[8] "should" now appears in the November 2015 version of the Code and the same point is highlighted by the use of square brackets below.

Necessity and proportionality

48. Within Chapter 2 the EI Code contains detailed guidance on the requirements of necessity and proportionality and how these statutory requirements are to be applied in the EI context. At §§2.6-2.8 it states:

> "*2.6 Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not alone render the most intrusive actions proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.*
>
> *2.7 The following elements of proportionality should therefore be considered:*
>
> - *balancing the size and scope of the proposed interference against what is sought to be achieved;*
> - *explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;*
> - *considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;*
> - *evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented.*
>
> *2.8 It is important that all those involved in undertaking equipment interference operations under the 1994 Act are fully aware of the extent and limits of the action that may be taken under the warrant in question.*"

49. Consequently the EI Code draws specific attention to the need to balance the seriousness of the intrusion against the need for the activity in operational and investigative terms, including taking into account the effect on the privacy of any other person who may be affected i.e. other than the subject of the operation. The EI Code is also very clear that it is important to consider all reasonable alternatives and to evidence what other methods were considered and why they were not implemented.

Collateral intrusion

50. The EI Code also highlights the risks of collateral intrusion involved in equipment interference and provides guidance on how any such issues should be approached, including the need to carry out an assessment of the risk of collateral intrusion. At §§2.9-2.12 it states:

> "*2.9 Any application for a section 5 warrant should also take into account the risk of obtaining private information about persons who are not subjects of the equipment interference activity (collateral intrusion).*
>
> *2.10 Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the equipment interference activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved.*

2.11 All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the Secretary of State fully to consider the proportionality of the proposed actions."

51. In addition the EI Code makes clear at §2.12 that where it is proposed to conduct equipment interference activity specifically against individuals who are not intelligence targets in their own right, interference with the equipment of such individuals should not be considered as collateral intrusion but rather as "*intended intrusion"* and that:

> "*Any such equipment interference activity should be carefully considered against the necessity and proportionality criteria as described above*."

Reviewing warrants

52. At §§2.13-2.15 the Code sets out certain requirements for reviewing warrants and states as follows:

> "*2.13 Regular reviews of all warrants should be undertaken to assess the need for the equipment interference activity to continue. The results of a review should be retained for at least three years (see Chapter 5). Particular attention should be given to the need to review warrants frequently where the equipment interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.*
>
> *2.14 In each case, unless specified by the Secretary of State, the frequency of reviews should be determined by the member of the Intelligence Services who made the application. This should be as frequently as is considered necessary and practicable.*
>
> *2.15 In the event that there are any significant and substantive changes to the nature of the interference and/or the identity of the equipment during the currency of the warrant, the Intelligence Services should consider whether it is necessary to apply for a fresh section 5 warrant.*"

General best practices

53. The EI Code gives guidance on general best practice to be followed by the Intelligence Services when making applications for warrants covered by the Code. At §2.16 those requirements are:

> "• *applications should avoid any repetition of information;*
> • *information contained in applications should be limited to that required by the 1994 Act;*
> • *where warrants are issued under urgency procedures (see Chapter 4), a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the applicant and authorising officer as a priority. There is then no requirement subsequently to submit a full written application;*
> • *where it is foreseen that other agencies will be involved in carrying out the operation, these agencies should be detailed in the application; and*
> • *warrants should not generally be sought for activities already authorised following an application by the same or a different public authority."*

54. In addition, the EI Code indicates that it is considered good practice that within each of the Intelligence Services, a designated senior official should be responsible for:

"• the integrity of the process in place within the Intelligence Service to authorise equipment interference;
- *compliance with the 1994 Act and this code;*
- *engagement with the Intelligence Services Commissioner when he conducts his inspections; and*
- *where necessary, overseeing the implementation of any post inspection action plans recommended or approved by the Commissioner.*" (see §2.17)

Legally privileged and confidential information

55. Chapter 3 of the Code contains detailed provisions on legally privileged and confidential information which it is intended to obtain or which may have been obtained through equipment interference.

Procedures for authorising equipment interference under s. 5

56. Chapter 4 of the EI Code sets out the general procedures to be followed for authorising equipment interference activity under s. 5 of the ISA. In that Chapter, §§4.1-4.4 outline the statutory scheme under the ISA. At §4.5 of the code, attention is drawn to the need to consider whether the equipment interference operation might also enable or facilitate a separate covert surveillance operation, in which case a directed or intrusive surveillance authorisation might need to be obtained under Part 2 of RIPA (as addressed in the Covert Surveillance and Property Interference Code).

57. In terms of applications for a s. 5 warrant, the EI Code contains a checklist of the information which each issue or renewal application should contain. At §4.6 it states:

"*An application for the issue or renewal of a section 5 warrant is made to the Secretary of State. Each application should contain the following information:*

- *the identity or identities, where known, of those who possess or use the equipment that is to be subject to the interference;*
- *sufficient information to identify the equipment which will be affected by the interference;*
- *the nature and extent of the proposed interference, including any interference with information derived from or related to the equipment;*
- *what the operation is expected to deliver and why it could not be obtained by other less intrusive means;*
- *details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected.*
- *whether confidential or legally privileged material may be obtained. If the equipment interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege or confidential personal information, but it is likely that such knowledge will nevertheless be acquired during the operation, the application should identify all steps which will be taken to mitigate the risk of acquiring it;*
- *details of any offence suspected or committed where relevant;*
- *how the authorisation criteria (as set out at paragraph 4.7 below) are met;*
- *what measures will be put in place to ensure proportionality is maintained (e.g. filtering, disregarding personal information);*
- *where an application is urgent, the supporting justification;*
- *any action which may be necessary to install, modify or remove software on the equipment;*
- *in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results.*"

58. At §4.7-§4.9 of the EI Code the statutory tests for the issuing of a s. 5 warrant are highlighted, together with the statutory requirements for any urgent authorisation of a s. 5 warrant.

Renewals and cancellations of warrants

59. At §§4.10-4.11 and §§4.12-4.13 of the EI Code the provisions of the ISA addressing the renewals and cancellations of warrants are summarised.

Keeping of records

60. In Chapter 5 of the EI Code provision is made for centrally retrievable records of warrants to be kept for at least three years. At §5.1 it states:

"*The following information relating to all section 5 warrants for equipment interference should be centrally retrievable for at least three years:*

- *the date when a warrant is given;*
- *the details of what equipment interference has occurred;*
- *the result of periodic reviews of the warrants;*
- *the date of every renewal; and*
- *the date when any instruction was given by the Secretary of State to cease the equipment interference.*"

61. In the latest version of the EI Code, these requirements are expanded and §5.1 states:

"*The following information relating to all section 5 warrants for equipment interference should be centrally retrievable for at least three years:*

- ***all applications made for warrants and for renewals of warrants;***
- *the date when a warrant is given;*
- ***whether a warrant is approved under urgency procedures;***
- ***where any application is refused, the grounds for refusal as given by the Secretary of State;***
- *the details of what equipment interference has occurred;*
- *the result of periodic reviews of the warrants;*
- *the date of every renewal; and*
- *the date when any instruction was given by the Secretary of State to cease the equipment interference."*

(items in bold are new requirements in this latest version of the Code)

Handling of information and safeguards

62. Chapter 6 of the EI Code provides important guidance on the processing, retention, disclosure deletion and destruction of any information obtained by the Intelligence Services pursuant to an equipment interference warrant and makes clear that this information may include communications content and communications data as defined in section 21 of RIPA (§6.1).

63. At §6.2 the EI Code states:

"*The Intelligence Services must ensure that their actions when handling information obtained by means of equipment interference comply with the legal framework set out in the 1989 and 1994 Acts (including the arrangements in force under these Acts), the Data Protection Act 1998 and this code, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with this legal*

framework will ensure that the handling of information obtained by equipment interference continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards against abuse."

64. At §§6.6-6.11 of the EI Code key safeguards are set out in the EI Code in terms of the dissemination, copying, storage and destruction of any information obtained as a result of equipment interference. In particular it is stated:

"***Dissemination of information***

6.6 ***The number of persons to whom any of the information is disclosed, and the extent of disclosure, must be limited to the minimum necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes described in paragraph 6.5.*** *This obligation applies equally to disclosure to additional persons within an Intelligence Service, and to disclosure outside the service. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: information obtained by equipment interference must not be disclosed to any person unless that person's duties are such that he needs to know about the information to carry out those duties. In the same way only so much of the information may be disclosed as the recipient needs; for example if a summary of the information will suffice, no more than that should be disclosed.*

6.7 ***The obligations apply not just to the Intelligence Service that obtained the information, but also to anyone to whom the information is subsequently disclosed.*** *In some cases this may be achieved by requiring the latter to obtain the originator's permission before disclosing the information further. In others, explicit safeguards may be applied to secondary recipients.*

Copying

6.8 ***Information obtained by equipment interference may only be copied to the extent necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes described in paragraph 6.5. Copies include not only direct copies of the whole of the information, but also extracts and summaries which identify themselves as the product of an equipment interference operation. The restrictions must be implemented by recording the making, distribution and destruction of any such copies, extracts and summaries that identify themselves as the product of an equipment interference operation.***

Storage

6.9 ***Information obtained by equipment interference, and all copies, extracts and summaries of it, must [should] be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store such information securely applies to all those who are responsible for the handling of the information.***

Destruction

6.10 ***Communications content, communications data and other information obtained by equipment interference, and all copies, extracts and summaries thereof, must [should] be marked for deletion and securely destroyed as soon as they are no longer needed for the functions or purposes set out in paragraph 6.5. If such***

information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid."

Personnel security

6.11 ***In accordance with the need-to-know principle, each of the Intelligence Services must ensure [should] that information obtained by equipment interference is only disclosed to persons as necessary for the proper performance of the Intelligence Services' statutory functions. Persons viewing such product will usually require the relevant level of security clearance.*** *Where it is necessary for an officer to disclose information outside the service, it is that officer's responsibility to ensure that the recipient has the necessary level of clearance."* (emphasis added)

65. At §§6.4-6.5 the importance of these safeguards is emphasised, together with the need to ensure that each of the Intelligence Services has **internal arrangements** in force for securing that the safeguards are satisfied, which arrangements should be made available to the Intelligence Services Commissioner. In particular it is stated:

"*6.4 Paragraphs 6.6 to 6.11 provide guidance as to the safeguards which must be applied by the Intelligence Services to the processing, retention, disclosure and destruction of all information obtained by equipment interference. Each of the Intelligence Services must ensure that there are internal arrangements in force, approved by the Secretary of State, for securing that these requirements are satisfied in relation to all information obtained by equipment interference.*

6.5 These arrangements should be made available to the Intelligence Services Commissioner. The arrangements must ensure that the disclosure, copying and retention of information obtained by means of an equipment interference warrant is limited to the minimum necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes set out in section 2(2)(a) of the 1989 Act and sections 2(2)(a) and 4(2)(a) of the 1994 Act. Breaches of these handling arrangements must be reported to the Intelligence Services Commissioner as agreed with him."

Application of the code to equipment interference pursuant to section 7 of the 1994 Act

66. In Chapter 7 of the EI Code it is made clear that "*GCHQ must [should] as a matter of policy*[9] *apply the provisions of this code in any case where equipment interference is to be, or has been, authorised pursuant to section 7 of the 1994 Act in relation to equipment located outside the British Islands*" (§7.1).

67. Consequently, save as expressly specified in Chapter 7 of the EI Code, all of the provisions of the EI Code, including the important safeguards regarding the processing, retention, disclosure deletion and destruction of any information obtained via equipment interference, apply equally to equipment interference authorised pursuant to s. 7 of the ISA. That is made expressly clear in §7.2 which states:

> "*GCHQ and SIS must [should] apply all the same procedures and safeguards when conducting equipment interference authorised pursuant to section 7 as they do in relation to equipment interference authorised under section 5."*

68. In addition, Chapter 7 of the EI Code provides specific additional guidance for s. 7 equipment

[9] And without prejudice to arguments as to the applicability of the ECHR, as made clear in footnote 17 of the draft Code and footnote 18 of the November 2015 version.

interference authorisations under the ISA.

69. In terms of the general basis for lawful activity under s. 7 of the ISA, the EI Code states at §§7.3-7.6:

> "*7.3 An authorisation under section 7 of the 1994 Act may be sought wherever members of SIS or GCHQ, or persons acting on their behalf or in their support, conduct equipment interference in relation to equipment located outside the British Islands that would otherwise be unlawful. This includes cases where the act is done in the British Islands, but is intended to be done in relation to apparatus that is or is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus.*
>
> *7.4 If a member of SIS or GCHQ wishes to interfere with equipment located overseas but the subject of the operation is known to be in the British Islands, consideration should be given as to whether a section 8(1) interception warrant or a section 16(3) certification (in relation to one or more extant section 8(4) warrants) under the 2000 Act should be obtained in advance of commencing the operation authorised under section 7. In the event that any equipment located overseas is brought to the British Islands during the currency of the section 7 authorisation, and the act is one that is capable of being authorised by a warrant under section 5, the interference is covered by a 'grace period' of 5 working days (see section 7(10) to 7(14)). This period should be used either to obtain a warrant under section 5 or to cease the interference (unless the equipment is removed from the British Islands before the end of the period).*
>
> *7.5 An application for a section 7 authorisation should usually be made by a member of SIS or GCHQ for the taking of action in relation to that service. Responsibility for issuing authorisations under section 7 rests with the Secretary of State.*
>
> *7.6 An authorisation under section 7 may be specific to a particular operation or user, or may relate to a broader class of operations. Where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of equipment interference must [should] be sought from a designated senior official (see paragraphs 7.11 to 7.14).*"

70. At §§7.7-7.8 and §§7.9-7.10 the EI Code sets out the statutory tests for s. 7 authorisations, together with the provisions of the statutory scheme dealing with urgent authorisations. At §7.7 the EI Code makes clear that:

> "*Each application should contain the same information, as far as is reasonably practicable in the circumstances, as an application for a section 5 equipment interference warrant.*"

71. Guidance on the types of authorisations under s.7 of the EI Code is also provided at §§7.11-7.14. In particular this provides guidance on any s. 7 authorisations which relate to a broad class of operations. At §§7.11-7.12 it states:

> "*7.11 An authorisation under section 7 may relate to a broad class of operations. Authorisations of this nature are referred to specifically in section 7(4)(a) of the 1994 Act which provides that the Secretary of State may give an authorisation which inter alia relates to "acts of a description specified in the authorisation". The legal threshold for giving such an authorisation is the same as for a specific authorisation.*

7.12 Where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of equipment interference must be sought from a designated senior official. In any case where the equipment interference may result in the acquisition of confidential information, authorisation must be sought from an Annex A approving officer. Where knowledge of matters subject to legal privilege may be acquired, the Annex A approving officer must apply the tests set out at paragraph 3.4 to 3.7 (and "Secretary of State" should be read as "Annex A approving officer" for these purposes).

72. For GCHQ an 'Annex A approving officer' means a Director of GCHQ (see Annex A on page 30).

73. In addition §§7.13-7.14 provide guidance on all internal applications for approval, including the need to ensure that such approvals are proportionate and are subject to periodic review at least every 6 months, or more frequently depending on the sensitivity of the operation. Those paragraphs state:

"7.13 The application for approval must [should] set out the necessity, justification, proportionality and risks of the particular operation, and should contain the same information, as and where appropriate, as an application for a section 5 equipment interference warrant. Before granting the internal approval, the designated senior official or Annex A approving officer must [should] be satisfied that the operation is necessary for the proper discharge of the functions of the Intelligence Service, and that the taking of the action is proportionate to what the action seeks to achieve. The designated senior official or Annex A approving officer must consult the Foreign and Commonwealth Office or seek the endorsement of the Secretary of State for any particularly sensitive operations.

7.14 All internal approvals must [should] be subject to periodic review at least once every 6 months to ensure the operations continue to be necessary and proportionate. The approvals for particularly sensitive operations should be reviewed more frequently, depending on the merits of the case."

74. As to renewals and cancellations of s. 7 authorisations, the statutory requirements are set out at §§7.15-7.17.

Oversight by the Intelligence Services Commissioner

75. In §§8.1-8.2 of the EI Code the important role of the Intelligence Services Commissioner in the use of the powers under the ISA is emphasised. In particular §8.2 states:

"*It is the duty of any member of the Intelligence Services who uses these powers to comply with any request made by the Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions. Such persons must also report any action that is believed to be contrary to the provisions of the 1994 Act to the Commissioner.*"

The Covert Surveillance and Property Interference Code ('the Property Code")

76. The Covert Surveillance and Property Interference Code ('the Property Code') provides guidance on entry on and interference with property by public authorities under s. 5 of the ISA (see the Code at §1.2).

77. Like the EI Code it was issued pursuant to s. 71 of RIPA. It was originally published in 2002 (called the 'Covert Surveillance Code of Practice') and a revised version was issued in 2010 (called the 'Covert Surveillance and Property Interference Revised Code of Practice'), with a further revised version published on 10 December 2014.

78. The Respondents have set out below the key provisions in the 2010/2014 version of the Code and in the 2002 version.

79. The changes as between the 2010 and the 2014 version of the Code are immaterial in terms of property interference activity by the Intelligence Services i.e. save for a few changes of paragraph number, the 2014 version did not alter the provisions relevant to these proceedings.

The 2010/2014 Property Code

80. Chapter 3 of the Code contains general rules on authorisations, *inter alia*, under s. 5 of the ISA. In particular guidance is given as to the requirement of proportionality. At §§3.3-3.7 the Code states:

> *"3.3 The ... 1994 Act stipulate[s] that the person granting an authorisation or warrant for ... interference with property, must believe that the activities to be authorised are necessary on one or more statutory grounds.*
>
> *3.4 If the activities are deemed necessary on one of more of the statutory grounds, the person granting the authorisation or warrant must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.*
>
> *3.5 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.*
>
> *3.6 The following elements of proportionality should therefore be considered:*
> - *balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;*
> - *explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;*
> - *considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;*
> - *evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.*
>
> *3.7 It is important therefore that all those involved in undertaking... interference with property under the ... 1994 Act are fully aware of the extent and limits of the authorisation or warrant in question.*"

81. Consequently the Code draws specific attention to the need to balance the seriousness of the intrusion against the need for the activity in operational and investigative terms, including taking into account the effect on the privacy of any other person who may be affected i.e.

other than the subject of the operation. The Code is also very clear that it is important to consider all reasonable alternatives and to evidence what other methods were considered and why they were not implemented.

82. The question of collateral intrusion is also directly addressed in §§3.8ff of the Code. At §3.11 it states:

"*Where it is proposed to conduct ... property interference specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such ... property interference activity should be carefully considered against the necessity and proportionality criteria as described above (paragraphs 3.3-3.8).*"

83. As to the procedures to be followed for reviewing authorisations, the Code states at §§3.22-3.24 (these appear as §§3.23-3.25 in the 2014 version of the Property Code):

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

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

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

84. The Code highlights best working practices which are to be followed by all public authorities with regard to all activities covered by the Code at §§3.27ff (§3.28 in the 2014 version of the Property Code). At §3.28 it states:

3.28 Furthermore, it is considered good practice that within every relevant public authority, a senior responsible officer should be responsible for:
• the integrity of the process in place within the public authority to authorise ... property or wireless telegraphy;
• compliance with ...this code;
• engagement with the Commissioners and inspectors when they
conduct their inspections, and where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

85. Chapter 4 of the Code contains special provisions on legally privileged and confidential information (see in particular §§4.10-4.15 and §§4.22-4.31).

86. Chapter 7 of the Code contains authorisation procedures for property interference. This specifically addresses authorisations for property interferences by the Intelligence Services. At §§7.36-7.38 it states:

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

7.37 The intelligence services should provide the same information as other agencies, as and where appropriate, when making applications for the grant or renewal of property warrants.

7.38 Before granting a warrant, the Secretary of State must:

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

The reference in §7.37 above to "the same information as other agencies" meant that, as and where appropriate §7.18 of the Code should be followed which provided:

7.18 Applications to the authorising officer for the granting or renewal of an authorisation must be made in writing (unless urgent) by a police officer, Revenue and Customs officer, SCDEA officer, a member of SOCA or an officer of the OFT and should specify:

• the identity or identities, where known, of those who possess the property that is to be subject to the interference;
• sufficient information to identify the property which the entry or interference with will affect;
• the nature and extent of the proposed interference;
• the details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why the intrusion is justified;
- *details of the offence suspected or committed;*

• how the authorisation criteria (as set out above) have been met;
• any action which may be necessary to maintain any equipment, including replacing it;
• any action which may be necessary to retrieve any equipment;
• in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and
• whether an authorisation was given or refused, by whom and the time and date on which this happened.

87. In terms of renewals and cancellations of warrants by the Intelligence Services, §§7.39-7.42 of the Code state as follows:

"*7.39 A warrant shall, unless renewed, cease to have effect at the end of the period of six*

months beginning with the day on which it was issued (if the warrant was issued under the hand of the Secretary of State) or at the end of the period ending with the fifth working day following the day on which it was issued (in any other case).

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

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

7.42 The person who made the application to the Secretary of State must apply for its cancellation, if he is satisfied that the warrant no longer meets the criteria upon which it was authorised..."

88. Chapter 8 of the Code provides that certain records shall be kept of property interferences which are authorised. At §8.3 it states:

"8.3 The following information relating to all authorisations for property interference should be centrally retrievable for at least three years:
• the time and date when an authorisation is given;
• whether an authorisation is in written or oral form;
...
• every occasion when entry on or interference with property or with wireless telegraphy has occurred;
• the result of periodic reviews of the authorisation;
• the date of every renewal; and
• the time and date when any instruction was given by the authorising officer to cease the interference with property or with wireless telegraphy."

89. In Chapter 9 of the Code guidance is given as to the handling of material obtained through property interference. §9.3 of the Code addresses the retention and destruction of material and states as follows:

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

90. In addition the Code states at §9.7 that, in relation to the Intelligence Services:

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

91. Finally Chapter 10 of the Code highlights the oversight which is provided by the Intelligence Services Commissioner on the use of the powers under the ISA. At §10.2 it states:

"*The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within ... the 1994 Act by ... GCHQ*."

The 2002 Property Code

92. Chapter 2 of the Code contains general rules on authorisations, *inter alia*, under s. 5 of the ISA. Paragraph 2.10 specifically makes clear that the guidance on necessity and proportionality and on collateral intrusion in this part of the Code must be taken into account when applying for authorisations or warrants for entry onto or interference with property or with wireless telegraphy.

93. Consequently guidance is given as to the requirements of necessity and proportionality. At §§2.4-2.5 the Code states:

"2.4 Obtaining an authorisation under the...1994 Act will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place.

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

94. The question of collateral intrusion is addressed in §§2.6-2.9 of the Code. In particular the following passages are relevant:

2.6 ...the authorising officer should take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

2.7 An application...should include an assessment of the risk of collateral intrusion. The authorising officer should take this into account, when considering the proportionality of the [property interference].

95. In §2.19 of the Code it addresses obligations on the heads of the Intelligence Services and states:

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

96. In Chapter 3 of the Code provisions were set out addressing special rules on authorisations including on communications subject to legal privilege (§3.3ff) and communications involving confidential personal information and confidential journalistic material (§3.10ff).

97. Chapter 6 addressed the authorisation procedures for entry onto or interference with property under, *inter alia*, the ISA, including the duration of property warrants.

6.32 Before granting a warrant, the Secretary of State must:

- *think it necessary for the action to be taken for the purpose of assisting the relevant agency in carrying out its functions;*

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

6.34 A warrant shall, unless renewed, cease to have effect if the warrant was under the hand of the Secretary of State, at the end of the period of ***six months*** *beginning with the day on which it was issued. In any other case, at the end of the period ending with the* ***second working day*** *following that day.*

6.35 If at any time before the day on which a warrant would cease to have effect the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, he may by an instrument under his hand renew it for a period of ***six months*** *beginning with that day. The Secretary of State shall cancel a warrant if he is satisfied that the action authorised by it is no longer necessary."*

98. In addition §6.36 makes clear that:

6.26 The intelligence services should provide the same information as the police, as and where appropriate, when making applications, requests for renewal and requests for cancellation of property warrants.

99. Consequently the provisions at §6.9ff of the Code which set out the authorisation procedures for the police are also to be applied by the Intelligence Services as and where appropriate. These provisions include a detailed list of matters which should be included in any application for an authorisation – see §6.12 of the Code, including:

- *the identity or identities of those to be targeted (where known);*
- *the property which the entry or interference with will affect;*
- *the identity of the individuals and/or categories of people, where known, who are likely to be affected by collateral intrusion;*
- *details of the offence planned or committed;*
- *details of the intrusive surveillance involved;*
- *how the authorisation criteria...have been met;*
- *any action which may be necessary to retrieve any equipment used in the surveillance;*
- *in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and*
- *whether an authorisation was given or refused, by whom and the time and date."*

100. Finally Chapter 7 of the Code highlights the oversight which is provided by the Intelligence Services Commissioner on the use of the powers under the ISA. At §10.2 it states:

"*The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within ... the 1994 Act by ... GCHQ*."

<u>The HRA</u>

101. Art. 8 of the ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) of the HRA. Art. 8, set out in Sch. 1 to the HRA, provides as follows:

> *"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *(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 prevent of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others*."

102. Art. 10 of the ECHR, which is similarly a Convention right (and which is similarly set out in Sch. 1 to the HRA), provides:

> *"(1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
> *(2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."*

103. By s. 6(1):

> "*It is unlawful for a public authority to act in a way which is incompatible with a Convention right*."

104. Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking any activity that interferes with Art. 8 rights, GCHQ must (among other things) act proportionately and in accordance with law. In terms of equipment interference activity, the HRA applies at every stage of the process i.e. from authorisation, through to the obtaining, retention, handling and any disclosure/dissemination of such material.

105. S. 7(1) of the HRA provides in relevant part:

> "*A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may—*
> *(a) bring proceedings against the authority under this Act in the appropriate court or tribunal ....*"

The DPA

106. Each of the Intelligence Services is a data controller (as defined in s. 1(1) of the DPA) in relation to all the personal data (as defined in s. 1(1) of the DPA) that it holds. Insofar as the obtaining of an item of information by any of the Intelligence Services amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data.

107. Consequently as a data controller, GCHQ is in general required by s. 4(4) of the DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) of the DPA, which exempt personal data from (among other

things) the data protection principles if the exemption "*is required for the purpose of safeguarding national security*". By s. 28(2) of the DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services (including GCHQ) are available on request. Those certificates certify that personal data that are processed in performance of the Intelligence Services' functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from the sixth data protection principle). Thus the certificates do not exempt the Intelligence Services (including GCHQ) from their obligation to comply with the fifth and seventh data protection principles, which provide:

"*5. Personal data processed*[10] *for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …*

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."[11]

108. Accordingly, when GCHQ obtains any information as a result of any property interference which amounts to personal data, it is obliged:

(a) not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained / used; and

(b) to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question.

The OSA

109. A member of the Intelligence Services commits an offence if "*without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services*": s. 1(1) of the OSA. A disclosure is made with lawful authority if, and only if, it is made in accordance with the member's official duty (s. 7(1) of the OSA). Thus, a disclosure of information by a member of GCHQ that is *e.g.* in breach of the relevant "arrangements" (under s. 4(2)(a) of the ISA) will amount to a criminal offence. Conviction may lead to an imprisonment for a term not exceeding two years and/or a fine (s. 10(1) of the OSA).

110. Further, a member of the Intelligence Services commits an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of any of those services, as a person in his position may reasonably be expected to take. See s. 8(1) of the OSA, as read with s. 1(1). Conviction may lead to an imprisonment for a term not exceeding three months and/or a fine (s. 10(2) of the OSA).

Oversight mechanisms

111. There are three principal oversight mechanisms in respect of the equipment interference regime:

[10] The term "processing" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

[11] The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

(a) The Intelligence Services Commissioner

(b) The ISC; and

(c) The Tribunal.

The Intelligence Services Commissioner

112. As highlighted in the relevant Code, the Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within the ISA by the Intelligence Services including GCHQ.

113. The Prime Minister is under a duty to appoint a Commissioner (see s. 59(1) of RIPA). By s. 59(5), the person so appointed must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government. The Commissioner is currently Sir Mark Waller.

114. Under s. 59(7) of RIPA, the Commissioner must be provided with such staff as are sufficient to ensure that he can properly carry out his functions. Those functions include those set out in s. 59(2), which provides in relevant part:

> "*…the [Commissioner] shall keep under review, so far as they are not required to be kept under review by the Interception of Communications Commissioner-*
> *(a) the exercise by the Secretary of State of his powers under sections 5 to 7 of... the Intelligence Services Act 1994...*"

115. A duty is imposed on, among other persons, every person holding office under the Crown to disclose and provide to the Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions: s. 60(1) of RIPA.

116. In practice, the Commissioner visits each of the Intelligence Services and the main Departments of State twice a year. Representative samples of warrantry paperwork are scrutinised, including the paperwork for s. 5 and/or s.7 ISA warrants/authorisations. Written reports and recommendations are produced after his inspections of the Intelligence Services. The Commissioner also meets with the relevant Secretaries of State.

117. S. 60 of RIPA imposes important reporting duties on the Commissioner. (It is an indication of the importance attached to this aspect of the Commissioner's functions that reports are made to the Prime Minister.)

118. The Commissioner is by s. 60(2) of RIPA under a duty to make an annual report to the Prime Minister regarding the carrying out of his functions. He may also, at any time, make any such other report to the Prime Minister as he sees fit (s. 60(3). Pursuant to s. 60(4), a copy of each annual report (redacted, where necessary under s.60(5)), must be laid before each House of Parliament. In this way, the Commissioner's oversight functions help to facilitate Parliamentary oversight of the activities of the Intelligence Services (including by the ISC). The Commissioner's practice is to make annual reports in open form, with a closed confidential annex for the benefit of the Prime Minister going into detail on any matters which cannot be discussed openly.

119. S. 58(5) grants the Commissioner power to make, at any time, any such other report to the Prime Minister on any other matter relating to the carrying out of his functions as he thinks fit.

120. In addition, the Commissioner is required by s. 59(3) to give the Tribunal:

"*…such assistance (including his opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require-*

(a) in connection with the investigation of any matter by the Tribunal; or

(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter."

121. The Tribunal is also under a duty to ensure that the Commissioner is apprised of any relevant claims / complaints that come before it: s. 68(3).

122. The Commissioner's oversight functions are supported by the record keeping obligations that are imposed as part of the equipment interference regime, see §8.3 of the Code.

123. It is to be noted that in the *Liberty/Privacy* judgment the Tribunal placed considerable emphasis on the important oversight which is provided by the Interception Commissioner (see in particular §§24, 44, 91, 92 121 and 139 of the judgment) and a similarly important role is provided by the Intelligence Services Commissioner in the present context.

The ISC

124. GCHQ is responsible to the Foreign Secretary,[12] who in turn is responsible to Parliament. In addition, the ISC plays an important part in overseeing the activities of the Intelligence Services. In particular, the ISC is the principal method by which scrutiny by Parliamentarians is brought to bear on those activities.

125. The ISC was established by s. 10 of the ISA. As from 25 June 2013, the statutory framework for the ISC is set out in ss. 1-4 of and Sch. 1 to the Justice and Security Act 2013 ("the JSA").

126. The ISC consists of nine members, drawn from both the House of Commons and the House of Lords. Each member is appointed by the House of Parliament from which the member is to be drawn (they must also have been nominated for membership by the Prime Minister, following consultation with the leader of the opposition). No member can be a Minister of the Crown. The Chair of the ISC is chosen by its members. See s. 1 of the JSA.

127. The executive branch of Government has no power to remove a member of the ISC: a member of the ISC will only vacate office if he ceases to be a member of the relevant House of Parliament, becomes a Minister of the Crown or a resolution for his removal is passed by the relevant House of Parliament. See §1(2) of Sch. 1 to the JSA.

128. The ISC may examine the expenditure, administration, policy and operations of each of the Intelligence Services: s. 2(1). Subject to certain limited exceptions, the Government (including each of the Intelligence Services) must make available to the ISC information that it requests in the exercise of its functions. See §§4-5 of Sch. 1 to the JSA. The ISC operates within the "ring of secrecy" which is protected by the OSA. It may therefore consider classified information, and in practice takes oral evidence from the Foreign and Home Secretaries, the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ, and their staff. The ISC meets at least weekly whilst Parliament is sitting. Following the extension to its statutory remit as a result of the JSA, the ISC is further developing its investigative capacity by appointing additional investigators.

129. The ISC must make an annual report to Parliament on the discharge of its functions (s. 3(1) of the JSA), and may make such other reports to Parliament as it considers appropriate (s. 3(2)

[12] The Director of GCHQ must make an annual report on the work of GCHQ to the Prime Minister and the Secretary of State (see s. 4(4) of the ISA).

of the JSA). Such reports must be laid before Parliament (see s. 3(6)). They are as necessary redacted on security grounds (see ss. 3(3)-(5)), although the ISC may report redacted matters to the Prime Minister (s. 3(7)). The Government lays before Parliament any response to the reports that the ISC makes.

130. The ISC sets its own work programme: it may issue reports more frequently than annually and has in practice done so for the purposes of addressing specific issues relating to the work of the Intelligence Services.

The Tribunal

131. The Tribunal was established by s. 65(1) of RIPA. Members of the Tribunal must either hold or have held high judicial office, or be a qualified lawyer of at least 7 years' standing (§1(1) of Sch. 3 to RIPA). The President of the Tribunal must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA).

132. The Tribunal's jurisdiction is broad. As regards the Equipment Interference regime, the following aspects of the Tribunal's jurisdiction are of particular relevance:

(a) The Tribunal has exclusive jurisdiction to consider claims under s. 7(1)(a) of the HRA brought against any of the Intelligence Services or any other person in respect of any conduct, or proposed conduct, by or on behalf of any of the Intelligence Services (ss. 65(2)(a), 65(3)(a) and 65(3)(b) of RIPA).

(b) The Tribunal may consider and determine any complaints by a person who is aggrieved by any conduct by or on behalf of any of the Intelligence Services which he believes to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system (ss. 65(2)(b), 65(4) and 65(5)(a) of RIPA).

133. Complaints of the latter sort must be investigated and then determined "by applying the same principles as would be applied by a court on an application for judicial review" (s. 67(3)).

134. Thus the Tribunal has jurisdiction to consider any claim against any of the Intelligence Services that it has obtained, interfered with or disclosed information emanating from interferences with property/equipment in breach of the ECHR. Further, the Tribunal can entertain any other public law challenge to any such alleged obtaining, interference with or disclosure of information.

135. Any person, regardless of nationality, may bring a claim in the Tribunal. Further, a claimant does not need to be able to adduce cogent evidence that some step has in fact been taken by the Intelligence Services in relation to him before the Tribunal will investigate.[13] As a result, the Tribunal is perhaps one of the most far-reaching systems of judicial oversight over intelligence matters in the world.

136. Pursuant to s. 68(2), the Tribunal has a broad power to require a relevant Commissioner (as defined in s. 68(8)) to provide it with assistance. Thus, in the case of a claim of the type identified in §134 above, the Tribunal may require the Intelligence Services Commissioner (see ss. 59-60 of RIPA) to provide it with assistance.

[13] The Tribunal may refuse to entertain a claim that is frivolous or vexatious (see s. 67(4)), but in practice it has not done so merely on the basis that the claimant is himself unable to adduce evidence to establish *e.g.* that the Intelligence Services have taken some step in relation to him. There is also a 1 year limitation period (subject to extension where that is "equitable"): see s. 67(5) of RIPA and s. 7(5) of the HRA.

137. S. 68(6) imposes a broad duty of disclosure to the Tribunal on, among others, every person holding office under the Crown.

138. Subject to any provision in its rules, the Tribunal may - at the conclusion of a claim - make any such award of compensation or other order as it thinks fit, including, but not limited to, an order requiring the destruction of any records of information which are held by any public authority in relation to any person. See s. 67(7).

INTERNAL ARRANGEMENTS

139. GCHQ also has internal arrangements in relation to s.5 warrants and s.7 authorisations. These are set out below, with gisted passages underlined.

The Compliance Guide

140. The Compliance Guide is a document which is made available electronically to all GCHQ staff. The electronic version of the Compliance Guide was made available to staff in late 2008 and there have been no substantive changes since then, although it has been amended in minor ways to ensure that it remains up to date. It comprises mandatory policies and practices which apply to all GCHQ operational activity and has been approved by the Foreign Secretary and the Interception of Communications Commissioner. The Compliance Guide requires all GCHQ operational activity, including CNE activity, to be carried out in accordance with three core principles. These are that all operational activity must be:

a) Authorised (generally through a warrant or equivalent legal authorisation);

b) Necessary for one of GCHQ's operational purposes; and

c) Proportionate.

141. These principles, and their application to specific activities conducted by GCHQ, are referred to throughout the Compliance Guide. They are also specifically referred to in the additional CNE-specific internal guidance referred to below. In short, they are core requirements which run through all the guidance which applies to GCHQ's operational activities, including CNE.

142. The section of the Compliance Guide which specifically concerns CNE states that authorisation is required under the ISA in order to address the liability which most CNE operations would normally attract under the Computer Misuse Act 1990. The requirement for a section 5 warrant for CNE operations on computers in the UK is made clear. Section 5 warrants are also addressed in the Compliance Guide as follows:

"*A Secretary of State must approve a new ISA s.5 warrant. Renewal is required after six months. In an emergency, a new temporary warrant may be issued by a GCHQ official of appropriate seniority if a Secretary of State has expressly authorised its use."*

Section 5 Guidance

143. GCHQ also has separate specific internal guidance governing applying for, renewing and cancelling section 5 warrants ("the Section 5 Guidance"). The Section 5 Guidance, application forms and warrant templates were updated following a visit of the Intelligence Services Commissioner (Sir Mark Waller) in June 2013. During that visit the Intelligence Services Commissioner acknowledged that GCHQ gave due consideration to privacy issues, but commented that he would like to see greater evidence of this reflected in warrants and submissions, in particular in relation to why the likely level of intrusion, both into the target's

privacy and the collateral intrusion into the privacy of others, was outweighed by the intelligence to be gained. In response, GCHQ updated its s.5 (as well as its s.7) application forms, warrant templates and guidance to advise staff on the type and level of detail required. At his next inspection in December 2013, the Intelligence Services Commissioner was provided with these documents and stated that he was content with the actions that had been taken.

144. The Section 5 Guidance makes clear the nature of the activity which is authorised by a s.5 warrant:

*"**ISA Section 5 guidance***

ISA warrants

Warrants issued under the Intelligence Services Act (ISA) authorise interference with property (eg equipment such as computers, servers, routers, laptops, mobile phones, software, intellectual property etc) or wireless telegraphy."

145. The geographical, functional and temporal limits of a s.5 warrant are also set out:

*"A **section 5 warrant** authorises interference with property or wireless telegraphy in the British Islands[14]...It may only be issued on grounds of National Security or the Economic Well-Being of the UK. A section 5 warrant is signed by a Secretary of State and is valid for 6 months from the date of signature, at which point the warrant should be renewed or cancelled."*

146. The guidance mirrors the requirements of s.5(2)(a) and (b) of the ISA. First, it makes clear that the proposed CNE action must be **necessary**:

"Part I. – to be completed by the relevant GCHQ team
The intelligence case should be fit for purpose for signing by a Secretary of State, avoiding unnecessary jargon and technical terminology. The case should include:

- *the intelligence background;*
- *the priority of the target within the priorities framework as endorsed by JIC[15] and NSC[16];*
- *an explanation of why the proposed operation is necessary;*
- *a description of any other agency involvement in working the target;*
- *the intelligence outcome(s) the proposed operation is expected to produce."*

147. The requirement that the proposed CNE action be **proportionate** is also made clear:

"As CNE techniques are by nature intrusive, an explanation of how proportionality will be maintained should be given. Key points to consider include:

- *the expected degree of invasion of a target's privacy and whether any personal or private information will be obtained;*
- *the likelihood of collateral intrusion, ie invading the privacy of those who are not targets of the operation, eg family members;*
- *whether the level of intrusion is proportionate to the expected intelligence benefit;*
- *a description of the measures to be taken to ensure proportionality."*

148. The Section 5 Guidance stipulates that each request for a warrant, or warrant renewal, must

[14] Both instances of underlining in this quotation are in the original.
[15] Joint Intelligence Committee.
[16] National Security Council.

have a sponsor of an appropriately senior level:

*"**Requesting a new Section 5***
Requests for new warrants and renewals must be sponsored by an appropriately senior official, who must be satisfied that the proposed operation is justified, proportionate and necessary."

149. The Section 5 Guidance requires that, once completed, the warrant request must be returned to its "sponsor" for consideration of whether it passes the test set out in s.5(2)(a) and (b) of the ISA, before being signed and sent to the relevant personnel:

"The form is then returned to the sponsor to consider whether, in light of the CNE input, they can recommend to the Secretary of State that the operation is justified, proportionate and necessary, and that they are aware of the risk. If so, they should sign and date the form and send it to the relevant personnel."

150. The Section 5 Guidance also explains that the process is completed by the preparation of a formal submission and a warrant instrument. These are reviewed by GCHQ Legal Advisers and the sponsor, then sent for signature to the relevant Department, which will follow its own internal procedures before the documents are passed to the Secretary of State for consideration. Once the warrant has been signed, relevant personnel will be informed that the operation can go ahead.

151. A designated form must be filled out when a section 5 warrant is sought. The specified information reflects the requirements of the guidance on section 5 warrants, and includes the following:

a) Under "Intelligence Case"

"why is CNE necessary and why can the expected intelligence not be gained by other less intrusive means[17]?"

"what intelligence the operation is expected to deliver

b) Under "Degree of intrusion, including collateral intrusion"

"how far will the operation intrude on the privacy of the target? Is the operation likely to obtain personal or private information?

to what extent will the operation affect those not of operational interest (eg could the individual's computer be used by family members, friends or colleagues who are not targets of the operation)?

how will the intelligence gained justify the expected level of intrusion?

what measures will be put in place to ensure proportionality is maintained."

(c) Under "Recipients of Product":

"where within GCHQ is the product of the CNE operation to be sent?"

[17] Underlining in the original.

(d) Finally, the Request must be authorised by the appropriately senior GCHQ official, who must, inter alia, certify that *"The proposed CNE operation is justified, proportionate and necessary".*

Renewals of s.5 warrants

152. The Section 5 Guidance also details the procedure for renewals of section 5 warrants. This requires specific attention to be paid, *inter alia*, to whether the operation is still justified, necessary and proportionate at the time of the renewal:

*"**Section 5 renewal process***
A reasonable period before a warrant is due to expire, the relevant personnel will request a case for renewal from the relevant personnel, copying the sponsor and include a copy of the previous submission. The analyst should confirm with the sponsor that renewal is required, and if so, provide the relevant personnel with a business case by the specified deadline. This should include:

- *an update of the intelligence background, ensuring it accurately reflects the current context of the warrant;*
- *details of any developments and intelligence gained since the warrant was issued/last renewed – this **must** address any expectations highlighted in the previous submissions;*
- *a review of the level of intrusion, based on the evidence of the activity authorised by the warrant;*
- *a review and, if necessary, update of the political aspects of the risk assessment;*

The relevant team should provide the following information:

- *any updates on technical progress made since the warrant was last renewed*
- *an updated operational plan – again, this **must** address specific actions or plans laid out in the previous submission*
- *any updates to the risk assessment.*

Again, the relevant personnel may need to work with the originator and the relevant team to strengthen the renewal case, and will also consult the Legal Advisers before providing a copy to the sponsor for final review. When the sponsor is content that the submission is accurate and demonstrates that the operation is still justified, necessary and proportionate, the relevant personnel will submit the renewal application to the relevant Department for signature."

Cancellation of s.5 warrants

153. The Section 5 Guidance also addresses cancellation of warrants, making clear that as soon as warrants are no longer required they should be cancelled:

"If a warrant is no longer required, it should be cancelled. If not renewed or cancelled, the warrant will expire on the date specified and the activity will no longer be authorised.

It is good practice to cancel warrants as soon as the requirement for the operation has ceased.

Section 5 cancellation process
When a warrant is no longer required, the analyst should send the relevant personnel a short explanation of the reason for the cancellation. When the team conducting the operation confirms that the operation is fully drawn down, the relevant personnel will draft a letter based on this feedback and submit it, with a cancellation instrument, to the issuing Department for signature (usually by a senior official rather than the Secretary of State)."

Section 7 Guidance

154. GCHQ's guidance which governs applying for, renewing and cancelling section 7 authorisations/internal approvals is set out both in the Compliance Guide (in the section dealing with authorisations) and in separate internal guidance ("the Section 7 Guidance"). The process set out in the Section 7 Guidance has been subject to the scrutiny and advice of the Intelligence Services Commissioner who has confirmed that he is content with the process.[18]

155. The Section 7 Guidance requires any CNE activities overseas to be carried out pursuant to a s.7 authorisation in order for such activities to be lawful under domestic law. Authorisations may either be specific to a particular operation or to a broad class of operation:

*"**ISA Section 7 guidance***

ISA authorisations

An ISA s7 authorisation given by the Secretary of State is the legal instrument that removes criminal liability in the UK for GCHQ actions overseas which might otherwise be an offence in UK law. Such an authorisation is also capable of removing any civil liability in the UK that might arise as a result of GCHQ's actions overseas. GCHQ primarily uses s7 authorisations for CNE operations. An ISA s7 authorisation may be specific to a particular operation or target, or may relate to a broad class of operations…"

156. The Section 7 Guidance sets out the 'class authorisations' signed by the Secretary of State under section 7 of the ISA which are used by GCHQ for the majority of its active internet-related operations. In respect of the authorisations relevant to CNE the Section 7 Guidance states that it:

"*permits interference with computers and communication systems overseas and removes liability under the Computer Misuse Act 1990 for interference with target computers or related equipment overseas (for this sort of activity, it is the location of the target computer which is relevant). The interference includes CNE operations."*

157. The Section 7 Guidance also stipulates that such authorisations need to be renewed every six months, and assert the vital importance of providing information to the Secretary of State to justify any renewal:

"Class authorisations are signed by the Foreign Secretary and need to be renewed every six months. Relevant personnel in GCHQ are responsible for overseeing the renewal process. Prior to expiry of the authorisations, they will ask analysts to briefly (re)justify the necessity and proportionality of continuing to rely on all extent section 7 internal approvals for which they are the lead, as well as asking for feedback on the outcomes of operations conducted. Providing feedback to the Foreign Secretary on the value of operations conducted under the class authorisations is crucial in justifying their renewal."

158. The requirement, in addition to a section 7 class authorisation, for a section 7 approval for a

[18] In addition to the Intelligence Services Commissioner's suggestions in his June 2013 inspection, and his approval of GCHQ's consequent changes in his December 2013 inspection, during a visit in December 2014 GCHQ presented to and discussed with the Intelligence Services Commissioner, the "end to end" process regarding CNE operations using two operational case-studies. The class-authorisation, internal approvals and additions authorisations were considered. The Commissioner was then shown how CNE operators conduct the operations with a live demonstration of an operation. There was also a focus on the relevant forms (which were discussed in some detail). The Commissioner indicated that he was content with the format and the level of detail in the forms.

specific operation, and the procedure for obtaining such an approval, is set out both in the section of the Compliance Guide on CNE, and also in the Section 7 Guidance. The latter emphasises, *inter alia*, the importance of considering and setting out, in a request for a section 7 approval, why an operation against a target is necessary and proportionate, and the requirement that a copy of the signed approval be sent to the FCO:

*"**ISA section 7 internal approvals***
A condition of section 7 authorisations is that GCHQ operates an internal section 7 approval process to record its reliance on these authorisations. Before tasking the operational team to conduct CNE operations, analysts are required to complete a request form including a detailed business case described the necessity and proportionality of conducting operations against the targets. The request also sets out the likely political risk. The request must be endorsed by a senior member of the operational team before it is passed to an appropriately senior official for approval…A copy of the signed final version of the approval is sent to FCO for information."

159. The Section 7 Guidance explains the importance of this process, including the provision of signed approvals to the FCO, for ensuring that operations are necessary, justified and proportionate is again stressed:

"This process provides the necessary reassurance to FCO that operations carried out under the class authorisations are necessary, justified and proportionate."

160. Necessity (including why means other than a CNE operation could not be used) and proportionality (particularly with regard to the privacy of a target or any third party) are addressed in more detail under *"Section B – business case/necessity/proportionality":*

"The business case should…include:
- *the intelligence background;*
- *the priority in the priorities framework;*
- *an explanation of why the operations against the target set are necessary;*
- *the intelligence outcome(s) the proposed CNE activities are expected to produce."*

You should also consider the level of intrusion the proposed operations will involve and how proportionality will be maintained. Key points to consider include:
- *the expected degree of intrusion into a target's privacy and whether any personal or private information will be obtained;*
- *the likelihood of collateral intrusion, i.e. invading the privacy of those who are not targets, such as family members;*
- *whether the level of intrusion is proportionate to the expected intelligence benefit;*
- *any measures to be taken to ensure proportionality."*

161. The Section 7 Guidance makes clear, under "Completing the process" that the internal approval will then be provided to an appropriately senior GCHQ official for signature and for, *inter alia*, the setting of a review period for the internal approval:

"Based on all the information provided, relevant personnel will ensure that the section 7 internal approval is suitable for referral to an appropriately senior GCHQ official for signature. That official will review all the matters relevant to the application to satisfy himself that the proposed activity is justified, necessary and proportionate, including validating the assessment of political risk. He will also set the review period for the internal approval, which will be shorter for particularly sensitive operations."

162. The standard form used for seeking section 7 approvals reflects both the Section 7 Guidance

and the statutory criteria. In particular it sets out the following:

a) *"**Business case, including***
- *Intelligence background (to include brief details of what has been achieved from other accesses).*
- *What you expect to get from using CNE techniques against this target set & how the intelligence gained will justify the expected level of intrusion.*
- *Any timing factors or special sensitivities.*

…"

b) *"**Necessity, including***
- *The necessity of conducting CNE operations against this target set (an explanation of why the use of CNE techniques is necessary)."*

c) ***"Proportionality and consideration of intrusion into privacy, including***
- *The proportionality of conducting CNE operations against this target set (CNE operations are intrusive by nature, and are likely to obtain information which is personal and private). Confirm that you have assessed that the level of intrusion into privacy, including collateral intrusion, is justified and proportionate. Outline measures to be put in place to ensure proportionality is maintained."*

The term *"privacy"* is defined *"in the broadest sense to mean a state in which one is not observed or disturbed by others".*

163. The appropriately senior GCHQ official who must support any request for a section 7 approval has to certify, *inter alia*, that:

"Operations conducted under this approval are justified, proportionate and necessary."

164. The relevant form also makes clear that the request for an approval should be sent to the relevant personnel at request stage, review stage and cancellation stage. Where an addition to an approval is sought the relevant personnel must also be consulted.[19] As a matter of practice, and as required by the Section 7 Guidance, final versions of s.7 approvals are sent to the Foreign and Commonwealth Office. A monthly summary report which summarises new s.7 approvals, reviews of s.7 approvals and cancellations, and also attaches copies of new approvals, is also sent to the relevant senior official at the FCO.

165. The Section 7 Guidance also deals with the situation where there is a significant change to an existing approval, or when a new target is proposed with the result that an "addition" to an existing approval is required.

166. The "additions form" requires the same regard to be had to justification, necessity and proportionality as is required for an initial approval.

Review of s.7 internal approvals

167. Approvals must be reviewed, and upon each review consideration is required to be given to whether the operation is still necessary and proportionate, specifically having regard to issues of intrusion and privacy. The process of reviewing s.7 approvals is summarised in the Section 7 Guidance as follows:

[19] A reference to "relevant personnel" is to staff who are responsible for securing legal/policy approvals, checking the relevant risk assessments and maintaining compliance records.

*"**Reviewing section 7 internal approvals***

In addition to the reviews that are carried out in support of the renewal of the class authorisations when analysts are required to briefly (re)justify the necessity and proportionality of continuing to rely on all extant internal approvals for which they are the lead, there is a rolling programme of fully revalidating all extant section 7 internal approvals. This revalidation mirrors the process for obtaining a new internal approval: an updated business case (covering justification, necessity, proportionality and intrusion into privacy) is provided by the lead analyst; the operational team confirm that they are still operating within the risk thresholds set when the internal approval was signed; the endorser confirms that the assessment of the likely political risk is still correct; then continued operations may be approved and a new review date set if no significant changes have been made (or the review of the approval is passed to a GCHQ official of appropriate seniority."

168. The review and revalidation is held at intervals determined by the designated GCHQ senior official who originally signed the section 7 approval. These are more frequent for particularly sensitive operations. The Section 7 Guidance also sets out a procedure for recording the history of a section 7 approval from the original submission through to any review or cancellation:

"New review history and cancellation forms will be appended at each review point. The intention is to leave the original submission intact, so that there is an audit trail of what was originally submitted/approved. If there are any updates to be made, these will be included in the review history so that there is an ongoing record at each review of what was decided and why."

169. Thus the approval process, including any review, is recorded so that the history of and basis (including necessity and proportionality) for any approval, review or cancellation, is available for audit.

Cancellation of s.7 internal approvals

170. The Section 7 Guidance also stipulates the need to cancel internal approvals as soon as an operation is no longer needed:

*"**Cancelling a section 7 internal approval***
To show due diligence and as a condition of relying on the class authorisations, section 7 internal approvals should be cancelled when an operation is no longer needed. To help ensure that this happens, the relevant personnel will ask whether section 7 internal approvals are still needed as part of the class authorisation renewals process, and if so will seek a brief rejustification of the continuing necessity and proportionality. The number of approvals signed or cancelled is provided to the Foreign Secretary with the case for renewal.

It is important to cancel an internal approval as soon as it is no longer required.

When a section 7 internal approval is no longer required, the analyst should ask the operational team point of contact to cease operations and remove all tasking. The relevant personnel will not formally cancel the approval until the operational team confirms that the operation is fully drawn down."

171. The Section 7 Guidance therefore contains safeguards against section 7 approvals remaining in place where they are no longer necessary and/or proportionate.

Obtaining data

172. There are further safeguards in place to ensure that decisions by CNE operators to obtain data from implanted devices are lawful. In particular:

a) In addition to a formal process of training and examination which all CNE Operators have to undergo, all CNE operators must every two years also undertake advanced legalities training which is specific to active operations such as CNE (in addition to the basic legalities training which all staff are required to complete).

b) CNE operators can obtain legal advice at any time.

c) In addition, any data obtained in an operation will be available to the relevant intelligence analysts for that project, who in turn will be aware of the legal authorisation for the project, and will also have completed legalities training. The CNE section of the Compliance Guide provides guidance for intelligence for intelligence analysts requesting a particular document to be retrieved.

173. Thus, the obtaining of data is subject to the same requirements of necessity and proportionality as the initial process of obtaining an authorisation/warrant/approval.

Storage of and access to data

174. GCHQ also has policies for storage of and access to data obtained by CNE.

175. The section of the Compliance Guide concerning "Review and Retention" states that GCHQ treats "all operational data" (i.e. including that obtained by CNE) as if it were obtained under RIPA. It sets out GCHQ's arrangements for minimising retention of data in accordance with RIPA safeguards. This is achieved by setting default maximum limits for storage of operational data.

176. In addition GCHQ has a separate policy specifically concerning data storage and access. It defines different categories of data, and importantly ascribes specific periods for which different categories of data may be kept, as well as explaining how different categories of CNE data relate to the categories of operational data set out in the Compliance Guide.

177. Where CNE analysts identify material as being of use for longer periods than the stipulated limits, it can be retained for longer, subject to justification according to specific criteria.

178. Access to data is also subject to strict safeguards, which are set out in the Compliance Guide. CNE content may be accessed by intelligence analysts, but they must first demonstrate that such access is necessary and proportionate by completing a Human Rights Act ("HRA") justification. HRA justifications are recorded and made available for audit. CNE technical data relating to the conduct of CNE operations may only be accessed by a team of trained operators responsible for planning and running such operations.

179. GCHQ's policy on storage of and access to data also requires GCHQ analysts who are not in the CNE operational unit to justify access to CNE data on ECHR grounds (particularly necessity and proportionality). The justification must be recorded and available for audit.

Handling/disclosure/sharing of data obtained by CNE operations

180. Pursuant to GCHQ's Compliance Guide, the position is that all operational material is handled, disclosed and shared as though it had been intercepted under a RIPA warrant. The term "operational material" extends to all information obtained via CNE, as well as material obtained as a result of interception under RIPA.

181. The general rules, as set out in the Compliance Guide and the Intelligence Sharing and Release Policy which apply to the handling of operational material include, *inter alia*, a requirement for mandatory training on operational legalities and detailed rules on the disclosure of such material outside GCHQ and the need to ensure that all reports are disseminated only to those who need to see them.

a) Operational data cannot be disclosed outside of GCHQ other than in the form of an intelligence report.

b) Insofar as operational data comprises or contains confidential information (e.g. journalistic material) then any analysis or reporting of such data must comply with the *"Communications Containing Confidential Information"* section of the Compliance Guide. This requires GCHQ to have greater regard to privacy issues where the subject of the interception might reasonably assume a high degree of privacy or where confidential information is involved (e.g. legally privileged material, confidential personal information, confidential journalistic information, communications with UK legislators). GCHQ must accordingly demonstrate to a higher level than normal that retention and dissemination of such information is necessary and proportionate.

Training

182. In addition to the training referred to at paragraphs 172(a) and 181 above, GCHQ does provide some training for analysts on particular CNE activities, which reiterates the substance of the Section 7 Guidance. GCHQ is currently in the process of revising the training referred to at paragraph (172(c)) to incorporate more detail on CNE.