Home Office

Equipment Interference

DRAFT Code of Practice

Autumn 2016

Equipment Interference

DRAFT Code of Practice

Pursuant to Schedule 7 to the Investigatory Powers Act 2016

Autumn 2016

Contents

1 Introduction

Background

1.1 This code of practice provides guidance on the use by the Security and Intelligence Agencies (Security Service, Secret Intelligence Service ("SIS"), and Government Communications Head Quarters ("GCHQ"), law enforcement agencies and Defence Intelligence ("the equipment interference agencies") of the Investigatory Powers Act 2016 ("the Act") to authorise equipment interference. It provides guidance on when a warrant under the Act is required to carry out equipment interference, the procedures that must be followed before equipment interference can be carried out, and on the examination, retention, destruction and disclosure of any information obtained by means of the interference.

1.2 The Act provides a statutory framework for authorising equipment interference when the European Convention of Human Rights ("the ECHR") and/or the Computer Misuse Act 1990 ("the CMA") are likely to be engaged. Chapter 2 of the code provide further guidance on the CMA, and when equipment interference warrants are required under the Act.

1.3 This code is issued pursuant to Schedule 7 of the Act, which provides that the Secretary of State shall issue one or more codes of practice about the exercise of functions conferred by virtue of the Act. This code replaces the previous equipment interference code of practice issued in 2015 which governed the Security and Intelligence Agencies' use of equipment interference.

1.4 This code is publicly available and should be readily accessible by members of any of the equipment interference agencies seeking to use the Act to authorise equipment interference.

1.5 For the avoidance of doubt, the guidance in this code takes precedence over any contrary content of an equipment interference agency's internal advice or guidance.

Effect of code

1.6 Paragraph 6 of Schedule 7 to the Act provides that all codes of practice issued under the Act are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal ("the IPT") established under the Regulation of Investigatory Powers Act 2000 ("RIPA"), or to a supervisory authority[1] exercising functions under the Act, it must be taken into account. The equipment interference agencies may also be required to justify, with regard to this code, the use of equipment interference warrants in general or the failure to use warrants where appropriate.

[1] A supervisory authority is the IPC or any other Judicial Commissioner: see paragraph 6 of Schedule 7 to the Act.

1.7 Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are not provisions of the code, but are included for guidance only. It is not possible for theoretical examples to replicate the level of detail to be found in real cases. Consequently, equipment interference agencies should avoid allowing superficial similarities with the examples to determine their decisions and should not seek to justify their decisions solely by reference to the examples rather than to the law, including the provisions of this code. The examples should not be taken as confirmation that any particular equipment interference agency undertakes the activity described; the examples are for illustrative purposes only.

Equipment interference to which this code applies

1.8 Part 5 of the Act provides for the issue of equipment interference warrants authorising interference with any equipment for the purpose of obtaining communications, equipment data or other information.

1.9 Equipment interference warrants may authorise both physical interference (e.g. covertly downloading data from a device to which physical access has been gained) and remote interference (e.g. installing a piece of software on to a device over a wired and/or wireless network in order to remotely extract information from the device).

1.10 An equipment interference warrant provides lawful authority to carry out the acquisition of communications stored in or by a telecommunications system. Where equipment interference activity amounts to interception of the content of communications in the course of their transmission (for example, live interception of an online video call), an interception warrant must be obtained under Part 2 or Chapter 1 of Part 6 of the Act.

1.11 Chapters 2 and 3 of this code provide a description of equipment interference activities and the circumstances when an equipment interference warrant is required, along with definitions of terms, exceptions and examples.

Basis for lawful equipment interference activity

1.12 The Human Rights Act 1998 gives effect in UK law to the rights set out in the 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.

1.13 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 equipment interference agencies 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[2]).

1.14 The use of equipment interference techniques may also necessarily involve interference with computers. Interfering with the functions of a computer or otherwise accessing it where there is no lawful authority to do so may, in certain circumstances, amount to a criminal offence. The offences related to unauthorised interferences with computers are set out in the CMA and are explained further in Chapter 2 of this code.

[2] Including equipment.

1.15 Part 5 and Chapter 3 of Part 6 of the Act provide a statutory framework under which equipment interference activities which engage the ECHR and/or would otherwise constitute an offence under the CMA can be authorised and conducted lawfully. The use of equipment interference warrants is mandatory in certain circumstances by virtue of section 11 of the Act and this code. Equipment interference agencies may choose to authorise equipment interference under the Act in other circumstances, but are not required to do so. Conduct which has lawful authority by virtue of an equipment interference warrant is treated as lawful for all other purposes.

2 Scope and definitions

Overview

2.1 Equipment interference warrants authorise interference with equipment for the purpose of obtaining communications, equipment data or other information and any conduct required to carry out authorised interference.

2.2 This chapter provides further guidance on the scope of equipment interference and relevant definitions, and on the circumstances where an equipment interference warrant is required for an equipment interference agency to undertake equipment interference activity.

Equipment interference

2.3 Equipment interference describes a range of techniques used by the equipment interference agencies that may be used to obtain communications, equipment data or other information from the equipment. The material so obtained may be used evidentially or as intelligence, or in some cases to test, maintain or develop equipment interference capabilities.

2.4 Equipment interference can be carried out either remotely or by physically interacting with the equipment. Equipment interference operations vary in complexity. At the lower end of the scale, an equipment interference agency may covertly download data from a subject's mobile device when it is left unattended, or an agency may use someone's login credentials to gain access to data held on a computer. More complex equipment interference operations may involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device.

Example 1: An equipment interference agency covertly downloads data from a device (such as a smart phone or laptop) either through direct access to the device itself (for example by access to USB ports) or by remotely installing software which enables material to be extracted.

Example 2: Key logging software is installed on a device by an equipment interference agency, making it possible to track every keystroke entered by users. The agency uses the key logger to track the keystrokes used when logging into a relevant website.

2.5 For the purposes of the Act, an equipment interference warrant can only be obtained for the purposes of obtaining communications, equipment data or other information.

2.6 Interference with equipment that is not for the purpose of acquiring communications, equipment data or other information will continue to fall within the definition of 'property interference' for the purposes of the Covert Surveillance and Property Interference Code of Practice. For example, disabling an alarm system to allow covert access to a building does not constitute equipment interference, although it may be necessary to interfere with the alarm system (equipment) to acquire equipment data in order to understand the operating system of the alarm system to enable it to be disabled. In such circumstances, the purpose of the interference is to defeat the alarm system and the acquisition of the equipment data is incidental. To the extent such activities would otherwise be unlawful, it should continue to be authorised under section 5 or 7 of Intelligence Services Act 1994 ("the 1994 Act") or Part 3 of the Police Act 1997 ("the 1997 Act").

2.7 This distinction has been drawn so that the Act can apply tailored safeguards, handling arrangements and oversight to activity where the purpose of the interference is to acquire communications, equipment data or other information from equipment. Different considerations will apply where the purpose of the interference is not to obtain communications, equipment data or other information, accordingly, the safeguards required differ to those applicable to equipment interference under the Act, and are provided through existing legislation.

Equipment

2.8 Equipment is defined in sections 127 and 182 of the Act. “Equipment" comprises any equipment producing “electromagnetic, acoustic or other emissions” and any device capable of being used in connection with such equipment. "Equipment" for these purposes is not limited to equipment which is switched on and/or is emitting signals but also includes equipment which is capable of producing such emissions.

2.9 The definition of equipment is technology neutral. Examples of the types of equipment captured by the definition include devices that are "computers" for the purposes of the CMA, such as desktop computers, laptops, tablets, smart phones, other internet-enabled or networked devices and any other devices capable of being used in connection with such equipment. Cables, wires and storage devices (such as USB storage devices, CDs or hard disks drives) are also covered as they can also produce "emissions" in the form of an electromagnetic field.

2.10 Equipment to which this code applies will vary as new technology is developed and produced. When reviewing this code of practice the Investigatory Powers Commissioner (“IPC”) should give particular consideration to this definition.

Equipment data

2.11 An equipment interference warrant may authorise the obtaining of communications, equipment data and other information. A warrant may provide for the obtaining of only equipment data. Equipment data comprises:

- systems data which is comprised in, included as part of, attached to or logically associated with the communications or information being acquired; and
- identifying data which is comprised in, included as part of, attached to or logically associated with the communications or information, which is capable of being logically separated from the remainder of the communication or item of information and which, once separated, does not reveal anything of what might reasonably considered to be the meaning (if any) of the communication or item information.

2.12 Equipment data is defined in sections 95 and 164 of the Act. Equipment data includes:

- Systems data:
  - Systems data includes two types of data. It includes the data which (when a communication is transmitted via a telecommunications system) is comprised in, attached to or logically associated with that communication and is necessary for the telecommunication system to transmit the communication. Second, there is other data comprised in, attached to or logically associated with communications or items of information which enable systems or services to function. While this second type of systems data is not necessary for a transmission system to transmit

a communication, it is also not content. These two types of data make up the broader set of information which is called systems data[3].

- Examples of systems data would be:
  - messages sent between items of network infrastructure to enable the system to manage the flow of communications;
  - router configurations or firewall configurations;
  - software operating system (version);
  - historical contacts from sources such as instant messenger applications or web forums;
  - alternative account identifiers such as email addresses or user IDs; and
  - the period of time a router has been active on a network.

- Identifying data:
  - A communication or item of information may include data which may:
  - be used to identify, or assist in identifying, any person, apparatus, system or service;
  - be used to identify any event; or
  - be used to identify the location of any person, event or thing.
  - In most cases this data will be systems data, however, there will be cases where this information does not enable or otherwise facilitate the functioning of a service or system and therefore is not systems data. Where such data, can be logically separated from the remainder of the communication or item of information and does not, once separated, reveal anything of what might reasonably be considered to be the meaning (if any) of any communication or item of information (disregarding any inferred meaning) it is identifying data.

- Examples of such data include:
  - the location of a meeting in a calendar appointment;
  - photograph information - such as the time/date and location it was taken; and
  - contact 'mailto' addresses within a webpage

Protected material

2.13 Protected material refers to material that is subject to particular access safeguards when acquired through bulk equipment interference and selected for examination using criteria referable to an individual known to be in the British Islands.

2.14 Protected material includes private information and the content of communications. Equipment data and non-private information (that is not a communication) are not protected material[4].

[3] Systems data that is necessary for the provision and operation of a service or system also includes the data necessary for the storage of communications and other information on relevant systems. Systems data held on a relevant system may be obtained via an equipment interference warrant under Part 5 or Chapter 3 of Part 6 of the Act.

[4] See section 179(9) of the Act.

Example: In the case of an email stored on a mobile phone, the message in the body of the email and the text in the subject line would not be equipment data (unless separated as identifying data). Accordingly, in the context of bulk equipment interference, this would be protected material and subject to the relevant safeguards set out in the Act when selected for examination using criteria referable to an individual known to be in the British Islands [5]*. Information associated with the stored email, such as the sender and recipient of the email or information about where the email is stored on the device, is equipment data and is not therefore protected material. In addition, information that is not private information which may be attached to the email, such as a publicly disseminated electronic magazine, would not be protected material*

Overseas-related communications, information and equipment data

2.15 Overseas-related communications, overseas-related information and overseas-related equipment data are defined in section 163 of the Act. The purpose of the definitions is to ensure that bulk equipment interference warrants are foreign focussed and are aimed at identifying communications and other information relating to individuals and entities outside the British Islands. The Security and Intelligence Agencies must accordingly ensure that the purpose of bulk equipment interference warrants is to obtain the communications, equipment data or other information of individuals or entities outside the British Islands.

Communications service provider

2.16 The obligations under Part 5 and Part 6 chapter 3 of the Act apply to telecommunications operators. Throughout this code, communications service provider ("CSP") is used to refer to a telecommunications operator.

2.17 A telecommunications operator is a person who offers or provides a telecommunication service to persons in the UK or who controls or provides a telecommunication system which is, (in whole or in part) in or controlled from the UK. This definition makes clear that obligations in the Act cannot be imposed on communications service providers whose equipment is not in or controlled from the UK and who do not offer or provide services to persons in the UK.

2.18 Section 237 of the Act defines 'telecommunications service' to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service); and defines 'telecommunications system' to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. The definition of 'telecommunications service' in the Act is intentionally broad so that it remains relevant for new technologies.

2.19 The Act makes clear that any service which consists of or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunications system are included within the meaning of 'telecommunications service'. Internet based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition.

[5] See section 179(9) of the Act.

2.20 The definition of a telecommunications operator also includes application and website providers but only insofar as they provide a telecommunication service. For example an online market place may be a telecommunications operator as it provides a connection to an application/website and because it provides a messaging service.

2.21 Telecommunications operators may also include those persons who provide services where customers, guests or members of the public are provided with access to communications services that are ancillary to the provision of another service, for example in commercial premises such as hotels or public premises such as airport lounges or public transport.

Restrictions on interference with equipment

Computer Misuse Act 1990

2.22 Interfering with the functions of a computer and accessing its data or its programs, where there is no lawful authority to do so, may in certain circumstances amount to a criminal offence. Sections 13 and 14 of the Act impose restrictions on equipment interference agencies, where it is considered that the proposed conduct would constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990 (CMA). Accordingly, it is important that equipment interference agencies understand when a CMA offence is likely to be committed.

2.23 "Computer" is not defined in the CMA; rather the Act relies on the ordinary meaning of the word in the relevant context. Some guidance is provided by section 69 of the Police and Criminal Evidence Act 1984, where the term was held to mean "a device for storing, processing and retrieving information". Such devices fall within the definition of "equipment" in sections 127 and 182 of the Act.

2.24 The offences relating to unauthorised interferences with computers are summarised below.

- Section 1: unauthorised access to computer material
- Section 2: unauthorised access with intent to commit or facilitate commission of further offences
- Section 3: Unauthorised acts with intent to impair, or with recklessness as to impairing the operation of a computer
- Section 3ZA: Unauthorised acts causing, or creating risk of, serious damage
- Section 3A: Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA.

2.25 The CMA provides that access will not be 'unauthorised' and an offence will not be committed if the conduct in question takes place pursuant to a relevant authorisation.

Mandatory use of targeted and bulk equipment interference warrants: security and intelligence agencies

2.26 Section 13 of the Act provides that it is mandatory for a security and intelligence agency to obtain an equipment interference warrant for the purpose of obtaining communications, equipment data or other information where a CMA offence would otherwise be committed and there is a British Islands connection.

2.27 A British Islands connection exists if:

- any of the conduct would take place in the British Islands (regardless of the location of the equipment which would, or may be, interfered with),
- the intelligence service believes that any of the equipment would, or may, be in the British Islands at some time while the interference is taking place, or
- a purpose of the interference is to obtain:
  - communications sent by, or to, a person who is, or is believed to be in the British Islands;
  - private information relating a person who is, or is believed to be in the British Islands; or
  - Equipment data which forms part of, or is connected with, the communications or private information outlined above.

Example: A member of an equipment interference agency installs a piece of software on a device located outside the British Islands by means of conduct effected within the UK. The software sends back information about the activities of the user of the target device. The service must obtain a targeted equipment interference warrant as the conduct would otherwise amount to unauthorised access to computer material contrary to the CMA and there is a British Islands connection by virtue of where the conduct takes place.

2.28 It is not mandatory under the Act for a security and intelligence agency to obtain a bulk equipment interference warrant other than when a CMA offence is committed and there is a British Islands connection. As a matter of policy, however, and without prejudice as to arguments regarding the applicability of the ECHR, when a security and intelligence agency plans to engage in activity for which it is able to obtain a bulk equipment interference warrant it should do so. The difference between targeted and bulk equipment interference is explained in paragraph 5.5.

2.29 In no circumstances may an equipment interference agency seek to circumvent the requirement to obtain a warrant by asking an international partner to undertake equipment interference on its behalf.

Restrictions on interference for law enforcement agencies

2.30 The Act provides a statutory framework under which law enforcement agencies may authorise targeted equipment interference to which the Act applies. Whether a targeted equipment interference warrant is available or required will depend on a number of factors, including whether the CMA is engaged, the appropriate law enforcement officer making the application, the nature of the equipment interference, where the interference is taking place and where the conduct takes place from.

2.31 By virtue of section 14 of the Act, law enforcement agencies may not, for the purpose of obtaining communications, private information or equipment data, obtain a property interference authorisation under Part 3 of the 1997 Act if the conduct would otherwise constitute an offence under the CMA. Where section 14 of the Act applies, a law enforcement officer must obtain a targeted equipment interference warrant under the Act to authorise equipment interference, unless the conduct is capable of being authorised under another law enforcement power (for example if the officer is exercising any powers of inspection, search or seizure or undertaking any other conduct that is authorised or required under an enactment or rule of law).

2.32 Accordingly, law enforcement officers will apply for an equipment interference warrant under this Act where the CMA is engaged and the conduct cannot be authorised under another law enforcement power. The CMA provides that access will not be ‘unauthorised’ if the conduct in question takes place pursuant to relevant authorisation.

Example: A law enforcement officer interferes with equipment by seizing it under powers arising from the Police and Criminal Evidence Act 1984 as relevant evidence in a criminal investigation. The officer's conduct is authorised by the 1984 Act and no equipment interference warrant is therefore required.

2.33 A law enforcement officer who is a member of a police force, the Ministry of Defence Police, the Police Investigations and Review Commissioner, the Independent Police Complaints Commission, the British Transport Police or the Police Services of Scotland or Northern Ireland may only be issued with a targeted equipment interference warrant if there is a British Islands connection (for definition of 'British Islands Connection' refer to paragraph 2.28). To further ensure that equipment interference activities conducted by these forces are focussed on investigations or operations within the British Islands, irrespective of whether there is a British Islands connection, these forces are prohibited by this code from obtaining an equipment interference warrant for interferences that takes place outside of the British Islands unless the subject of investigation is a UK national or is likely to become the subject of criminal or civil proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court. For example, such circumstances may arise where material is being acquired from equipment in the British Islands, but the equipment is subsequently temporarily taken outside the British Islands and the material continues to be captured[6].

Example: A law enforcement agency has obtained an equipment interference warrant authorising the acquisition of communications, information and equipment data from a subject's equipment. The subject temporarily leaves the British Islands with the relevant equipment. The law enforcement agency may continue to obtain material from the equipment while the target is outside the British Islands.

2.34 Law enforcement agencies other than those set out in 2.34 of this code may be issued with targeted equipment interference warrants regardless of whether there is a British Islands connection. Officers in these forces may therefore undertake equipment interference activities outside the British Islands. This division reflects the different work that the agencies are expected to carry out. For example, the National Crime Agency, ("NCA") may investigate crimes that originate outside of the British Islands but impact upon the UK. Conversely, a regional police force would be unlikely to routinely investigate crimes outside of the UK. In practice, should a regional police force need to investigate crimes taking place where there is no British Islands connection they will do so with the assistance of another agency, such as the NCA.

Non-mandatory use of targeted equipment interference warrants

Security and intelligence agencies

2.35 By virtue of the Act and this code, it is not mandatory for a security and intelligence agency to obtain an equipment interference warrant in two circumstances.

2.36 Firstly, a security and intelligence agency need not obtain an equipment interference warrant where there is a British Islands connection, but the conduct to be authorised does not constitute an offence under the CMA. An agency may obtain an equipment interference warrant in these circumstances, but need not do so if another authorisation route is available to provide a legal basis for the activity.

[6] See section 102 of the Act.

Example: An equipment interference agency interferes with a person's device with their consent, which enables a subject's communications and other information to be obtained by surveillance. If the agency considers that the access to the computer material would not be unauthorised and therefore would not constitute a CMA offence, it may obtain an intrusive surveillance authorisation under Part 2 of RIPA to authorise the surveillance. The agency will not require an equipment interference warrant.

2.37 Secondly, the Act does not require a security and intelligence agency to obtain an equipment interference warrant where there is no British Islands connection (even if the conduct to be authorised constitutes an offence under the CMA). Some equipment interference conducted outside of the British Islands will be small-scale and will often take place in difficult and hostile environments which are outside the control of the equipment interference agencies. The window of opportunity within which equipment operations can take place overseas is often small and unpredictable and it will not always be possible or safe to obtain prior individual authorisation for every act undertaken. In these circumstances it will be more appropriate to authorise the necessary conduct under section 7 of the 1994 Act.

2.38 However, the Act does not restrict the ability of an agency to apply for a targeted equipment interference warrant even where it is not mandatory under the Act. In particular this may include circumstances where the activity is taking place outside the British Islands in such a place that the relevant service considers that with regard to the ECHR it may be prudent to obtain a targeted equipment interference warrant. Such activity may include activity within British embassies, military bases and detention centres. Equipment interference agencies should also consider seeking an equipment interference warrant under the Act for targeted operations outside the British Islands if the subject of investigation is a UK national or is likely to become the subject of civil or criminal proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court.

2.39 In any case where communications, private information or equipment data are obtained under sections 5 or 7 of the 1994 Act, a security and intelligence agency must handle the material so obtained in accordance with the safeguards set out in Covert Surveillance and Property Interference Code. Compliance with these safeguards will ensure that the relevant service handles the material in accordance with safeguards equivalent to those set out in chapter 8 of this code[7].

Ministry of Defence

2.40 In common with other equipment interference agencies the Ministry of Defence will obtain an equipment interference warrant for any interference conducted by its civilian or service personnel which might amount to an offence under the CMA and have a connection to the British Islands where the circumstances are such that no defence to such a charge is clearly available (for example, in circumstances where combatant immunity might not apply).

Law enforcement agencies

2.41 Section 14 of the Act restricts the ability of law enforcement agencies to authorise interference with equipment under the 1997 Act. Where the purpose of the interference is to obtain communications, private information or equipment data, activity which was previously authorised under the 1997 Act should now be authorised under Part 5 of the Act, which is subject to enhanced safeguards tailored for this manner of activity.

[7] The Covert Surveillance and Property Interference Code will be updated prior to implementation of the Act.

2.42 As with existing property interference powers in the 1997 Act, this does not prohibit law enforcement agencies from using other powers available to them to access communications, equipment data or other information. In particular, law enforcement officers may continue to exercise their powers of inspection, search or seizure or undertake any other conduct amounting to interference for these purposes that is authorised or required under an enactment or rule of law - for example, where a law enforcement officer interferes with equipment by seizing it pursuant to a warrant issued under the Police and Criminal Evidence Act 1984 as relevant evidence in a criminal investigation. For the avoidance of doubt, and notwithstanding any other provisions of this code, an equipment interference warrant will not be required where the interference is authorised under another law enforcement power.

3 Equipment interference warrants - general rules

Overview

3.1 An equipment interference warrant under Part 5 or Chapter 3 of Part 6 of the Act will provide a lawful basis for an equipment interference agency to carry out equipment interference to obtain communications, equipment data or other information.

3.2 Responsibility for issuing targeted equipment interference warrants, and the purposes for which warrants may be issued, varies depending on the equipment interference agency applying for the warrant. Targeted examination warrants and bulk equipment interference warrants may only be issued by a Secretary of State to a security and intelligence agency. Targeted equipment interference warrants may be issued to the security and intelligence agencies and Defence Intelligence by the Secretary of State. In certain circumstances targeted equipment interference and targeted examination warrants may also be issued to the security and intelligence agencies by the Scottish Ministers. Targeted equipment interference warrants for law enforcement agencies are issued by a relevant law enforcement chief[8].

3.3 Where not otherwise specified this code will refer to the 'issuing authority' to include the Secretary of State, Scottish Minister or law enforcement chief where relevant.

Types of equipment interference warrant

3.4 The Act provides that three types of equipment interference warrant may be issued. Guidance on targeted equipment interference and targeted examination warrants is set out in Chapter 4 of this Code. Guidance on bulk equipment interference warrants is set out in Chapter 5 of this Code.

- A **targeted equipment interference warrant** described in section 94(2) of the Act authorises the person to whom it is addressed to secure interference with any equipment to obtain communications, equipment data or other information. The subject matter to which an equipment interference warrant may relate is specified in section 96.
- A **bulk equipment interference warrant** described in section 163 of the Act is a warrant which meets two conditions. First, it must authorise the person to whom it is addressed to secure interference with any equipment to obtain communications, equipment data or other information. Secondly, its purpose must be to obtain overseas-related communications, overseas-related information or overseas-related equipment data[9]. Material obtained under a bulk equipment interference warrant may only be selected for examination in accordance with the safeguards set out in section 168 of the Act including (where necessary) a targeted examination warrant.

[8] See Annex A for full table of law enforcement issuing authorities.

[9] See Chapter 3 and section 163 of the Act for the meaning of overseas-related communications, overseas-related private information or overseas-related equipment data.

- A **targeted examination warrant** described in section 94(9) of the Act authorises the person to whom it is addressed to carry out the selection for examination of protected material obtained under a bulk equipment interference warrant in breach of the prohibition in section 179(4) of the Act.

Equipment interference agencies

3.5 Only certain public authorities may apply for equipment interference warrants under the Act and only for the relevant specified purposes:

- Applications for targeted equipment interference warrants and targeted examination warrants may be made by or on behalf of the head of a security and intelligence agency on the grounds of national security, preventing or detecting serious crime[10] or the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security;
- Applications for targeted equipment interference warrants may be made by or on behalf of the Chief of Defence Intelligence on grounds of national security;
- Applications for targeted equipment interference warrants may be made by an appropriate law enforcement officer on the grounds of preventing or detecting serious crime or for certain law enforcement agencies, preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health[11].
- Applications for bulk equipment interference warrants may only be made by or on behalf of the head of a security and intelligence agency on grounds of national security, or on the grounds of national security and preventing or detecting serious crime and/or in the interests of the economic well-being of the UK (so far as those are also relevant to the interests of national security). At least one of the grounds for issuing a bulk equipment interference warrant must therefore be national security.

3.6 Warrants must be issued personally by a Secretary of State or the Scottish Ministers in the case of a security and intelligence agency, and by a Secretary of State in the case of Defence Intelligence. Equipment interference warrants for law enforcement agencies must be issued by a law enforcement chief to their relevant law enforcement officer (as listed in section 101 of the Act, see annex A).

3.7 The statutory purposes for which equipment interference warrants may be issued reflect the functions of the agency carrying out the equipment interference. Each of the equipment interference agencies must conduct equipment interference operations in accordance with their statutory or other functions, and the provisions of the Act.

[10] Serious crime is defined in section 239as crime that comprises an offence for which a person who has reached the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or which involves the use of violence, results in substantial financial gain - or is conduct by a large number of persons in pursuit of a common purpose.

[11] Use of equipment interference to prevent death or injury to a person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health will only be used in exceptional circumstances. In these circumstances equipment interference techniques will most likely be used to assist in locating vulnerable persons. Accordingly, the Act limits the use of equipment interference for this purpose to relevant agencies. The following persons may not apply for warrants for this purpose: Officers of The Competition and Markets Authority, officers of the Police Investigations and Review Commissioner, officers of Revenue and Customs and Immigration Officers. Section 96(2) of the Act restricts this power to the appropriate law enforcement agencies.

3.8 In the case of the Security and Intelligence Agencies:

- For the Security Service, the Security Service Act 1989 provides that the Service's functions are the protection of national security, the safeguarding of the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands and the provision of support to the police and other law enforcement authorities in the prevention and detection of serious crime;
- For the Secret Intelligence Service the 1994 Act provides that its functions are to obtain and provide information relating to the actions or intentions of persons outside the British Islands and to perform other tasks relating to the actions or intentions of such persons 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 in the interests of the economic well-being of the United Kingdom or in support of the prevention or detection of serious crime;
- In the case of the GCHQ, the 1994 Act provides, as relevant, that one of its functions is 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 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 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 in support of the prevention or detection of serious crime.

3.9 In the case of Defence Intelligence, as for the Ministry of Defence more generally, its functions derive from the prerogative. The Bill limits the use of equipment interference by the Ministry of Defence to matters concerning national security.

3.10 In the case of the NCA, the Crime and Courts Act 2013 confers functions on the NCA, Director General and NCA officers, which are collectively referred to as 'NCA functions'. The NCA functions are a 'crime reduction function', a 'criminal intelligence function' and a collection of other functions conferred by the 2013 Act and other enactments.

3.11 In the case of other law enforcement bodies, their functions derive from a mixture of statute and common law. For example, a police force is a number of individual constables, whose status derives from the common law, organised together in the interests of efficiency. A member of a police force, of whatever rank, when carrying out his duties as a constable acts as an officer of the Crown and a public servant. The primary duties of those who hold the office of constable are the protection of life and property, the preservation of the Queen's peace and the prevention and detection of criminal offences. In general terms, police forces are therefore responsible for the investigation of crime, collection of evidence and the arrest or detention of suspected offenders.

Incidental conduct

3.12 Where an equipment interference agency obtains an equipment interference warrant, the warrant also authorises any conduct necessary to undertake what is expressly authorised or required by the warrant (excluding conduct that constitutes the interception of live communications[12]).

[12] Live communication includes communications in the course of their transmission, but not stored communications.

3.13 This conduct may therefore include interference with associated or non-target equipment in order to obtain communications, equipment data or other information from the target equipment, providing that the conduct does not constitute live interception.

3.14 When applying for an equipment interference warrant the applicant should set out expressly any foreseeable incidental conduct that will be required to facilitate the equipment interference. It is possible that during the course of equipment interference activity further incidental conduct will be required that was not previously foreseen. This incidental conduct, and the obtaining of any material pursuant to this incidental conduct, is permissible and lawful for all purposes.

Example: An equipment interference agency has obtained a warrant to acquire communications and other relevant information from a target's device, which it anticipates gaining covert access to for a brief period of time. During the operation, the agency unexpectedly has access to two devices, and cannot determine whether one or both belong to the target. The agency is permitted to examine both using equipment interference techniques in order to clarify whether one or both belong to the target – this is incidental conduct, which may involve the obtaining of data from both devices. If one device is then found not to be connected to the target, the full equipment interference described in the warrant will not take place against that device and any data already obtained relating to that device will be deleted as soon as possible.

3.15 The warrant applicant, issuing authority and Judicial Commissioner should consider the incidental conduct that it may be necessary to undertake in order to do what is authorised on the face of the warrant. In cases where conduct is not clearly incidental, but may instead constitute a separate use of another power, the warrant applicant should consider whether a separate authorisation is required. If the status of incidental conduct remains uncertain the warrant applicant is may seek a separate authorisation (a combined authorisation may be appropriate).

Surveillance

3.16 The obtaining of communications or information authorised by a targeted equipment interference warrant includes obtaining those communications or information by surveillance. 'Surveillance' for these purposes includes monitoring, observing or listening to a person's communications or other activities, or recording anything that is monitored, observed or listened to. This could include intrusive surveillance (surveillance carried out in a residence or private vehicle) or directed surveillance (surveillance that is not in an intrusive setting, such as monitoring a subject in a public place).

3.17 A separate authorisation for surveillance under Part 2 of RIPA will not therefore be required providing the conduct comprising the surveillance is properly authorised by a targeted equipment interference warrant. The interference with privacy and property resulting from the equipment interference will be considered as part of the equipment interference authorisation.

3.18 In cases where an equipment interference agency wishes to obtain communications or information by surveillance under a targeted equipment interference warrant, the proposed activity should be set out in the application and be expressly authorised by the warrant.

3.19 By contrast, where the surveillance is not linked to the communications, equipment data or other information obtained from the equipment interference, this will not be capable of authorisation under a targeted equipment interference warrant.

3.20 For example, if an equipment interference agency wishes to conduct separate surveillance on the user of a device at the same time as the device itself is being subject to equipment interference, then this will not be considered as part of the equipment interference authorisation and appropriate surveillance authorisation must be obtained. In this situation a combined warrant may be appropriate (for information on combined warrants, see paragraph 4.80).

Interception

3.21 An equipment interference warrant cannot authorise conduct that would amount to an offence, under section 3(1), of unlawful interception of a communication in the course of its transmission (e.g. live interception of an online video call) except if the warrant authorises the obtaining of a communication stored in or by a telecommunication system. If an equipment interference agency wishes to conduct interception of communications other than stored communications, an interception warrant must be obtained under Part 2 or Chapter 1 of Part 6 of the Act (further guidance on interception warrants may be found in the Interception of Communications Code of Practice).

Example: An equipment interference agency wishes to conduct equipment interference on a device to acquire communications stored on the device and intercept video calls being made from the device, in the course of their transmission. The interception cannot be authorised by an equipment interference warrant, which includes as incidental conduct. An interception and equipment interference warrant must both be obtained (either as a combined warrant or separately).

Necessity and proportionality

3.22 The Act provides that the person issuing a **targeted equipment interference or targeted examination warrant** must consider that the warrant is necessary for one or more statutory purposes.

3.23 If the warrant is considered necessary for any of the purposes specified, the person issuing the warrant must also consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

3.24 In the case of a **bulk equipment interference warrant**, the Act provides that the Secretary of State must consider that the main purpose of the warrant is to obtain overseas-related communications, overseas-related information or overseas-related equipment data. The Secretary of State must also consider the warrant is necessary for one or more statutory purposes, and proportionate to what is sought to be achieved by the conduct.

3.25 The Secretary of State must consider that the selection for examination of any material obtained under the bulk warrant is necessary for one or more specified operational purposes, and that examination for the operational purposes is necessary for the statutory purposes specified in the warrant.

3.26 3.26 **For all equipment interference warrants** the issuing authority must also believe that the equipment interference is proportionate to what is sought to be achieved by that conduct. 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 material which is sought could reasonably be obtained by other less intrusive means.

3.27 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the interference against what is sought to be achieved;
- explaining how and why the methods to be adopted will minimise the risk of intrusion on the subject and others;
- whether the activity is an appropriate use of the legislation.
- whether there are any implications of the conduct authorised by the warrant for the privacy and security of other users of equipment and systems, including the internet, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation;
- evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented; and
- where a bulk equipment interference warrant is available, the safeguards set out in Chapter 3 of Part 6 of the Act.

3.28 In the case of warrants issued under sections 96(1) (g) and (2) (e) of the Act for the purposes of testing and training, proportionality should be considered by assessing the potential for, and seriousness of, intrusion into any affected persons' privacy against the benefits of carrying out the proposed testing or training exercise.

3.29 It is important that all those involved in undertaking equipment interference activity under the Act are fully aware of the extent and limits of the action that may be taken under the warrant in question.

Trade Unions

3.30 As set out in clauses 97, 98, 99 and 101 the fact that the information that would be obtained under the a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State, law enforcement chief or Scottish Ministers. Equipment interference agencies are permitted to apply for a warrant against members or officials of a trade union considered to be a legitimate intelligence target where that is necessary for one or more of the statutory purposes and proportionate to what is sought to be achieved.

Protection of the privacy and security of other users of equipment and systems, including the internet

3.31 Equipment interference agencies must not intrude into privacy any more than is necessary to carry out their functions or enable others to do so. To leave targets open to exploitation by others would increase the risk that their privacy would be unnecessarily intruded upon. Equipment interference activity must therefore be carried out in such a way as to appropriately minimise the risk of any increase in the; (i) likelihood or severity of any unauthorised intrusion into the privacy; or (ii) risk to the security, of users of equipment or systems (whether or not those equipment or systems are subject to the activities of the equipment interference agency.

Example: An equipment interference agency wishes to obtain communications from a device associated with an intelligence target which is connected to the internet through a network used by a range of individuals, not all of whom are of intelligence interest. Before issuing the warrant, the issuing authority must consider whether the proposed course of action would enable others to intrude into the privacy of users of the network, including those not of intelligence interest as well as the target. If this were to be the case, the issuing authority would (having first determined the necessity and proportionality of the activity proposed) need to be satisfied that the enabling of any such intrusion was minimised to the greatest extent possible.

3.32 In the case of warrants issued for the purposes of testing or training, interference should be carried out in such a way as to appropriately minimise the probability and seriousness of intrusion in to the privacy of any persons affected by, or in the vicinity of, the proposed activity.

3.33 Any application for an equipment interference warrant should contain an assessment of any risk to the security or integrity of systems or networks that the proposed activity may involve including the steps taken to appropriately minimise such risk according to paragraph 3.31. In particular, any application for an equipment interference warrant that relates to equipment associated with Critical National Infrastructure should contain a specific assessment of any risks to that equipment and the steps taken to appropriately minimise that risk. The issuing authority should consider any such assessment when considering whether the proposed activity is proportionate.

4 Targeted equipment interference warrants

4.1 This section applies to the two kinds of equipment interference warrants that may be issued under part 5 of the Act for the purpose of targeted equipment interference and examination with a warrant. These are:

- Targeted equipment interference warrants; and
- Targeted examination warrants (authorising the selection for examination of protected material obtained under a bulk equipment interference warrant).

4.2 A targeted equipment interference warrant described in section 94(2) of the Act authorises the person to whom it is addressed to secure interference with any equipment to obtain communications, equipment data or other information. A warrant may also authorise the disclosure of material obtained under the warrant.

4.3 Responsibility for the issuing of targeted equipment interference warrants, and the grounds on which the warrant may be issued, depends on the equipment interference agency applying for the warrant. With the exception of urgent warrants (see paragraph 4.50) all decisions to issue equipment interference warrants must be approved by a Judicial Commissioner before they are issued.

4.4 In the case of the **Security and Intelligence Agencies**, warrants must be issued by the Secretary of State on an application made by or on behalf of the head of a security and intelligence agency. The warrant must be necessary in the interests of national security, for the prevention or detection of serious crime or in the interests of the economic well-being so far as those interests are also relevant to the interests of national security[13]. Where the only equipment to be interfered with is in Scotland at the time the warrant is issued, and the warrant is necessary for the purpose of preventing or detecting serious crime, the warrant must be issued by a Scottish Minister.

4.5 In the case of **Defence Intelligence**, warrants must be issued by the Secretary of State on an application made by or on behalf of the Chief of Defence Intelligence. The warrant must be necessary in the interests of national security only.

4.6 In the case of **law enforcement**, warrants may be issued by a law enforcement chief on an application made by a person who is an appropriate law enforcement officer in relation to the chief. The warrant must be necessary for the purpose of preventing or detecting serious crime or for certain law enforcement agencies, preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

4.7 Targeted equipment interference warrants, when issued to the Security and Intelligence Agencies or the Ministry of Defence, are addressed to the person who submitted the application.

4.8 When targeted equipment interference warrants are issued to a law enforcement agency the Law Enforcement Chief can address the warrant to the applicant or to another person who is an appropriate law enforcement officer in relation to him. The person to who the warrant is addressed must be named or described in the warrant. Such a person must be an accountable individual but can be described by their relevant post within the law enforcement agency. This ensures the Law Enforcement Chief can address the warrant to the most applicable officer who is accountable for giving effect to the warrant

[13] A warrant will only be considered necessary on these grounds if the interference is necessary to obtain information relating to the acts or intentions of persons outside the British Islands.

4.9 Once issued a copy of the warrant may then be served on any person who may be able to provide assistance in giving effect to that warrant.

Format of warrant application

Targeted equipment interference warrants

4.10 An application for a targeted equipment interference warrant should contain the following information:

a. The background to the operation or investigation in the context of which the warrant is sought and what the operation or investigation is expected to deliver;

b. The subject-matter(s) of the warrant, to include the following information dependent on the subject-matter(s):

- Equipment belonging to, used by or in the possession of a particular person or organisation must name or describe that person or organisation;
- Equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on a particular activity, must name or describe as many of the persons as it is reasonably practicable to name or describe;
- Equipment used by or in the possession of more than one person or organisation where the warrant is for the purposes of a single investigation or operation, must describe the nature of the investigation or operation and name or describe as many of the persons or organisations as it is reasonably practicable to name or describe;
- Equipment in a particular location must include a description of the location;
- Equipment in more than one location where the interference is for the purpose of a single investigation or operation must describe the nature of the investigation or operation and describe as many of the locations as it is reasonably practicable to describe;
- Equipment which is being, or may be, used for the purposes of a particular activity of activities of a particular description must describe the activity or activities.
- Equipment which is being, or may be, used for testing and training purposes must describe the nature of the testing, maintenance or development of capabilities and/or a description of the training;

c. A description of any communications, equipment data or other information that is to be (or may be) obtained;

d. An outline of how obtaining the material will benefit the investigation or operation. The relevance of the material being sought should be explained along with any considerations which might be relevant to the consideration of the application;

e. Sufficient information to describe the type of equipment which will be affected by the interference;

f. A description of the conduct to be authorised as well as any conduct it is necessary to undertake in order to carry out what is expressly authorised or required by the warrant, including whether communications or other information is to be obtained by surveillance;

g. An assessment of the consequences and potential consequences of that conduct, including any risk of compromising the security of any equipment directly or indirectly involved with the interference and, in particular, whether this may enable further intrusion into privacy or impact upon Critical National Infrastructure;

h. In the case of thematic warrants, an assessment of whether it will be reasonably practicable to modify the warrant when the identities of the subjects become known and, if so, when such modifications are expected to occur. Where the warrant applicant believes it will not be reasonably practicable to modify the warrant as the identities of individuals, organisations or relevant locations become apparent they should set out the reasons for this.

i. The nature and extent of the proposed interference;

j. An explanation of why the equipment interference is considered to be necessary on one of the grounds set out in Part 5;

k. Consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, including where appropriate, explaining why less intrusive alternatives have not been or would not be as effective;

l. In the case of law enforcement agencies, the factors considered when determining if it is proportionate for the warrant to be issued to the appropriate law enforcement officer (see paragraph 4.35).

m. What measures will be put in place to ensure proportionality is maintained (for example, the methods by which the material collected will be processed to reduce collateral intrusion (e.g. through filtering or processing the material before any of it is examined), and these can be imposed as conditions on the granting of the warrant.)

n. Consideration of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why that intrusion is justified in the circumstances;

o. Whether the conduct is likely or intended to result in the obtaining of privileged or other confidential material and, if so, what protections it is proposed will be applied to the handling of the information so obtained; Where an application is urgent, the supporting justification;

p. In case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results, and an explanation of the collateral intrusion that has arisen to date and how this has been managed;

q. An assurance that all material obtained will be kept for no longer than necessary and handled in accordance with the safeguards required by section 122 of the Act and chapter 8 of this code.

4.11 Prior to submission to the person with responsibility for issuing the warrant, each application should be subject to a review within the agency seeking the warrant. This review will consider whether the application is for a purpose specified in the Act and whether the equipment interference proposed is both necessary and proportionate.

Targeted examination warrants

4.12 **A targeted examination warrant** described in section 94(9) of the Act authorises the person to whom it is addressed to carry out the selection for examination, in breach of the prohibition in section 179(4) of the Act, of protected material obtained under a bulk equipment interference warrant of an individual known for the time being to be in the British Islands.

4.13 Targeted examination warrants must be issued by the Secretary of State on an application made by or on behalf of the head of a security and intelligence agency. An application for a targeted examination warrant should contain the following information:

a. The background to the operation or investigation in the context of which the warrant is sought;

b. The subject-matter(s) of the warrant, to include the following information dependent on the subject-matter(s):

- A warrant that relates to a particular person or organisation must name or describe that person or organisation;
- A warrant that relates to a group of persons who share a common purpose or who carry on, or may carry on a particular activity, must name or describe as many of the persons as it is reasonably practicable to name or describe;
- Where a warrant relates to more than one person or organisation for the purposes of a single investigation or operation, it must describe the nature of the investigation or operation and name or describe as many of the persons or organisations as it is reasonably practicable to name or describe;
- A warrant that relates to testing and training activities must describe the nature of the testing, maintenance or development of capabilities and/or a description of the training;

c. A description of the protected material that is to be selected for examination;

d. An explanation of why the selection for examination is considered to be necessary on one of the grounds set out in Part 5;

e. Consideration of why the selection for examination to be authorised by the warrant is proportionate to what is sought to be achieved, explaining why less intrusive alternatives have not been or would not be as effective;

f. Consideration of any collateral intrusion and why that intrusion is justified in the circumstances;

g. Whether the selection for examination is likely or intended to result in the obtaining of privileged or other confidential material and, if so, what protections it is proposed will be applied to the handling of the information so obtained;

h. Where an application is urgent, the supporting justification;

i. An assurance that any protected material selected will be kept for no longer than necessary and handled in accordance with the safeguards required by section 122 of the Act (see chapter 8).

4.14 Prior to submission to the person with responsibility for issuing the warrant, each application should be subject to a review within the agency seeking the warrant. This review will consider whether the application is for a purpose specified in the Act and whether the equipment interference proposed is both necessary and proportionate.

Subject-matter and scope of targeted warrants

4.15 Section 96 sets out the subject-matter of targeted warrants and constrains what equipment can be described in the warrant or what protected material can be selected for examination; this section therefore sets the "scope" of a targeted warrant. Technically, any equipment may be interfered with or protected material selected for examination provided they fall within the warrant's scope. The subject-matter of equipment interference and examination warrants may be targeted or thematic.

Targeted warrants relating to a person, organisation or particular location

4.16 In many cases, equipment interference and examination warrants will relate to **targeted subjects**. Targeted subjects are described in sections 96(1)(a) and (d) and must comprise a particular person, organisation or a particular location. A "person" for these purposes may be an individual but also includes all legal persons, corporate or unincorporate. An "organisation" may additionally include entities that are not legal persons. This means, for example, that a warrant may relate to a particular company; the company is the "person" to which the warrant relates and the warrant will authorise interference with equipment belonging to, used by or in the possession of that company. There is no obligation to name any of the directors and employees etc. of the company in the warrant (see section 108(3)), although the warrant must describe the type of equipment to be interfered with which is likely to include equipment used by those persons. Similarly, in the case of an unincorporated body such as a partnership, a warrant may refer just to the partnership, but will authorise the interference with equipment used by members of that partnership.

4.17 In practice, an application for a targeted warrant of this nature falling within section 96(1)(a) or (d) is likely to be appropriate where the purpose of the warrant is to obtain intelligence about the legal person or organisation itself, rather than the individuals who are directors, employees or members of the company or organisation. The Act does not require the equipment interference agency to name or describe individuals within legal persons or organisations in the warrant; in many cases the identities of these individuals will be irrelevant to the intelligence being sought, their identities will not be known (or could only be ascertained by further interferences with privacy) and it would not provide a meaningful safeguard.

4.18 In the case of a particular location, this may relate to interfering with equipment in a building or a defined geographic area, where it is not technically feasible to identify individual users of the equipment. Whilst in this instance, activities of individuals may be of intelligence interest, it is the information gained from the equipment described in the warrant in which the equipment interference agency is interested.

Example 1

An organisation set up for procuring items relating to research is suspected of sourcing material for nuclear production in a country subject to UN sanctions. Further information is required about the organisation, the materials it sources, and the shipments of goods going out from the organisation. In this particular case, equipment interference is the least intrusive means of acquiring this information since the intelligence interest is in the organisation and its activities, not the individuals employed by the organisation who may not even be aware of what is going on. EI yields intelligence on the products being shipped to the country in question, confirming these are items that could only be used for nuclear production, and enabling the UN to take action.

Example 2

A military base is situated in a specific location known to be the centre for intercontinental ballistic missile research being undertaken by a country with hostile intentions against the UK. In order to track how the research is evolving and what types of systems are being developed, equipment interference is used to gather intelligence from that specific location. Intelligence reveals that the military base is in a state of readiness to test a recently developed missile and also exposes future plans for using the missile on an attack against the UK should the test be successful. The intelligence allows a UK military unit in the area to take action to safeguard UK national security.

Targeted thematic warrants

4.19 Targeted equipment interference warrants may cover equipment relating to more than one person, organisation or location; these are sometimes referred to as targeted 'thematic' warrants. Targeted thematic warrants can cover a wide range of activity; it is entirely possible for a thematic warrant to cover a wide geographical area or involve the acquisition of a significant volume of data, provided the strict criteria of the Act are met.

4.20 The Act provides for the way in which the subject of targeted warrants must be described; section 108(3) and (5) impose certain additional requirements as to what such warrants must specify. Where a targeted thematic warrant relates to equipment used by a group of persons who share a common purpose, for example, the warrant must name or describe as many of the persons as reasonably practicable. However, the list of persons does not set the scope of the warrant (which is the equipment used by the group) and therefore anyone who falls within the group as described will be within the scope of the warrant. Further guidance on targeted thematic warrants is set out below.

4.21 Section 95(1) of the Act contains the types of subject-matter to which a targeted warrant can relate. Targeted thematic warrants can cover the following subject matters:

a) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity (see section 95(1)(b)). For example, the warrant could authorise the interference with computer equipment associated with a group of individuals who are engaged in or supporting Islamist extremist attack planning in the UK;

b) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation (see section 95(1)(c)). For example, the warrant could authorise interference with the computer equipment of a number of companies that are being used as fronts for serious crime;

c) equipment in more than one location, where the interference is for the purpose of a single investigation or operation (see section 95(1)(e)). For example, the warrant could authorise interference with computer equipment in a number of locations which is believed to be being used in attempts to steal confidential commercial secrets of high financial value from UK technology firms, but where it may not be possible to identify the actor(s) behind the attack;

d) equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description (see section 95(1)(f)). For example, the warrant could authorise interference with computers which are all using the same paedophilia file sharing site;

e) equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information (see section 95(1)(g)). For example, the warrant could authorise the testing of a new technique to be deployed against computers to help ensure that the technique is effective. A warrant could be applied for where there is a risk of innocent users being impacted, for example if testing utilised a real world service. However, no such warrant would be needed for wholly internal laboratory testing.

f) equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment (see section 95(1)(h)). For example, the warrant could authorise training that is being carried out overseas to obtain equipment data from a number of devices owned and operated by the equipment interference agency. In order to obtain the data, these devices are connected to a live data environment which results in real world equipment data being stored on the device. In this example, a warrant is needed to authorise the use of equipment interference for training purposes. However, no such warrant would be required if the devices being targeted are owned and operated by the equipment interference agency and training is undertaken internally using data that has already been obtained under a previous warrant.

4.22 Providing the strict criteria in the Act for necessity and proportionality are met, there is no limit on the number of pieces of equipment relating to persons, organisations or locations which a targeted warrant may cover. The warrant does not need to detail the name or description of the persons, organisations or locations within the scope of a thematic warrant any more than is reasonably practicable at the time of the issue of the warrant. Due to the way in which equipment interference activity is conducted, in that it is targeting equipment rather than individuals, little may be known about the people using the equipment. This may be so, for example, because ubiquitous encryption is in use or the intelligence interest is in information contained on a device irrespective of who is using it. Similarly, the nature of EI techniques and the number of persons potentially covered by the subject-matter of the warrant, such as users of a web forum, would mean that where section 108 requires the warrant to name or describe as many of the persons as it is reasonably practicable to do so, this will often be a description of the class of persons falling within the subject matter, rather than individual names or descriptions. In addition, the nature of the operation or the group being investigated (e.g. a fast-moving operation where there is a threat to life or national security) might mean that it is not reasonably practicable to individually name all members of the group being investigated.

4.23 The thematic warrant application must, though, contain as much information as possible and be as specific as is necessary to enable the issuing authority to foresee the equipment to be covered and assess the scope of the warrant by reference to the group, persons or organisations, locations, activities or testing and training activity. This will ensure that the extent of the reasonably foreseeable interference with privacy caused by the equipment interference, or selection for examination, can be properly and fully assessed by the issuing authority. This enables the issuing authority, and the Judicial Commissioner in his/her review, to be satisfied as to the legality, necessity and proportionality of the conduct authorised. This will also assist those executing the warrant so that they are clear as to the scope of the warrant.

4.24 Where an equipment interference agency becomes aware of equipment belonging to, used by or in the possession of a new person, organisation or location within the authorised scope of a targeted thematic warrant and wishes to start interfering with that equipment, section 108 of the Act contains an ongoing duty to name or describe as many of the persons, organisations or locations which fall within the matter to which the warrant relates, as it is reasonably practicable to do so[14]. If it is reasonably practicable to do so, the new person, organisation or location must be added to the warrant through a modification, but a modification in these circumstances does not alter the scope of the warrant.

4.25 Section 108 only requires an equipment interference agency to seek a modification to add a name or description when it is reasonably practicable to do so. It may not be reasonably practicable, for example, in a fast moving threat to life operation or in a malware case where the agency is more interested in the pattern of behaviour of the actors, their methods and equipment rather than identifying persons involved. In no circumstances is it permitted to modify a warrant so as to authorise conduct falling outside the scope of the original warrant.

4.26 Whether or not it is reasonably practicable to modify a warrant to name or describe additional persons, organisations or locations will depend upon the operation to which the warrant relates. It is likely to be reasonably practicable to make such modifications in cases where there is not a requirement to act quickly due to a limited opportunity to carry out what is authorised by the warrant, or where the quantity and frequency of such modifications would not have a disproportionately adverse impact on the operations of the equipment interference agency.

4.27 For example, an equipment interference agency may have sought a thematic warrant relating to members of an organised crime group involved in the production of counterfeit travel documents. The warrant authorises interference with the equipment used by the group of persons carrying out the counterfeiting activity and names a number of individuals known to be involved, but also authorises interference with the equipment of as yet unidentified individuals that may be assisting the known criminals. If the agency discovers the identity of a new individual involved in the operation and wishes to interfere with equipment being used by that person, the warrant may be modified to include that individual's name or description. As the operation is not time critical and only one additional member has been identified it would be reasonably practicable to add the description of the newly identified individual to the warrant. This will assist the issuing authority in understanding which communications, equipment or other information are being obtained or selected, and will assist a judicial commissioner's oversight of the warrant.

[14] The duty to name or describe as many persons, organisations or locations as it is reasonably practicable to do so applies to warrants that have the subject matter of equipment belonging to, used by or in the possession of persons who form a group which shares a common purpose or who carry on, or may carry on, a particular activity; equipment used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation; and equipment in more than one location, where the interference is for the purpose of a single instigation or operation.

4.28 However, it may not be reasonably practicable to make such modifications, for example:

Example 1: An equipment interference agency is investigating a kidnapping and a warrant has been issued authorising the interference with equipment being used by members of the criminal group associated with the kidnapping. In this situation the time required to modify the warrant as new members of the criminal group are identified would adversely affect the agency's ability to carry out the authorised interference. The original warrant already authorises the required interference into the criminal group and the operation may therefore continue. If the warrant remains necessary for a longer period of time, it may become reasonably practicable to modify the warrant to include the identities listed in the warrant at a later date or upon renewal.

Example 2: An equipment interference agency is conducting an investigation into the pattern of behaviour of persons using a website to disseminate images of child sexual exploitation and a warrant has been issued authorising interference with equipment being used by more than one person to disseminate images via the website. In such a case naming or describing the persons involved in a meaningful way may not be possible due to the number of users of the website or without further unnecessary intrusion in to privacy. Furthermore, the frequency with which online identities change would make repeated modifications unreasonably constraining. The original warrant authorises interference with the equipment of the persons suspected of using the website for criminal purposes.

4.29 When issuing a thematic warrant it is important for the issuing authority to understand whether it is likely to be reasonably practicable to make modifications on the identities of individuals, organisations or relevant locations if they become apparent during the course of an operation.

4.30 The warrant application should therefore contain an assessment of whether it will be reasonably practicable to provide such modifications and, if so, when such modifications are expected to occur. Where the warrant applicant believes it will not be reasonably practicable to modify the warrant as the identities of individuals, organisations or relevant locations become apparent they should set out the reasons for this. This information will assist the issuing authority and Judicial Commissioner when considering if a warrant is necessary and proportionate.

4.31 Where it is not reasonably practicable for a thematic warrant to be modified when the identities of individuals, organisations or relevant locations become apparent over the course of an operation the warrant applicant must still provide the most up to date details in relation to the matters outlined in paragraph 4.10 upon renewal of the warrant. This will ensure that the issuing authority and Judicial Commissioner are able to fully assess whether the activity authorised by the warrant remains necessary and proportionate

4.32 If the issuing authority is able to foresee the extent of all of the interferences to a sufficient degree, including the degree of collateral material present at the time when examination of the material takes place, can therefore properly and fully assess necessity and proportionality and agrees that it is necessary and proportionate, then a thematic warrant can be granted. In such cases, the additional access controls which form an integral part of the bulk warrant regime are not required, given the issuing authority can adequately assess and address all of the relevant considerations at the time of issuing the warrant. By contrast, if it is not possible to so assess the necessity and proportionality of all of the interferences at the time of issuing the warrant, or the assessment is that in the circumstances it would not be proportionate to issue a thematic warrant, then a bulk warrant with its second stage authorisation process might be more appropriate if available.

4.33 In some instances it may not be possible to identify individual pieces of equipment or be specific about the nature of the equipment to be interfered with in advance, or there may be a technique that in itself carries out a specific small amount of interference, but enables access to the data that may already have been granted under an existing authorisation. In these cases the warrant should be specific about the technique and the circumstances in which the warrant is to be used. In such cases, the circumstances must be described in a way that enables the requirements of section 101 of the Act to be met.

4.34 There is an on-going duty to review the necessity and proportionality of warrants and to cancel them as necessary. This duty is especially important for thematic warrants given their scope is potentially wider.

Example 1: Intelligence has suggested that a number of unidentified criminal associates are planning to imminently commit a serious criminal offence. An equipment interference agency may wish to deploy equipment interference against the members of the group planning the offence. As the intelligence picture develops, the equipment interference agency expects to rapidly identify the potential offenders and the exact equipment that they are using. The agency obtains an equipment interference warrant relating to the equipment belonging to, or used by, a group of persons who are carrying on a particular activity (i.e. the planned offence) so they do not have to wait to get a new authorisation each time they identify a new member of the group and a new piece of equipment. However, the duty at section 107 would apply so that the warrant would need to be modified to add the name or description of as many of the persons if it was reasonably practicable to do so.

Example 2: Intelligence suggests that a Daesh-inspired cell dispersed across a small number of locations in the Middle East is plotting an imminent bomb attack against UK interests in the region. Interception reveals that the cell members are all using a unique technique to hide their identities online, known as an anonymisation package. After using equipment interference to obtain equipment data from a large number of devices in the specific locations, a search term ('selector') that is unique to the anonymisation package is applied to the data collected, ensuring that only data relating to the cell members is available for analysis. Using information from the initial analysis, the content from the cell members' devices is then obtained. As the cell members can be identified from their association to a specific, known anonymisation package, a targeted 'thematic' warrant is suitable.

Authorisation of a targeted equipment interference warrant

4.35 The person responsible for issuing the warrant may only issue a warrant under Part 5 if the person considers following tests are met:

- The warrant is necessary in the case of Security and Intelligence Agencies:[15]
  - In the interests of national security;
  - For the purpose of preventing or detecting serious crime;
  - In the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security. A warrant will only be considered necessary on this ground if the information relates to the acts or intentions of persons outside the British Islands.
- The warrant is necessary in the case of law enforcement agencies:
  - For the purpose of preventing or detecting serious crime;

[15] A single warrant can be justified on more than one of the grounds listed.

- in the case of law enforcement agencies listed in Part 1 of Schedule 6 of the Act
- for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

- The warrant is necessary in the case of Defence Intelligence:
  - In the interests of national security.
- **The conduct authorised by the warrant is proportionate to what it seeks to achieve.** In considering necessity and proportionality, the issuing authority must take into account whether the information sought could reasonably be obtained by other means.
- **There are satisfactory safeguards in place.** The issuing authority must consider that satisfactory arrangements are made for the purposes of the safeguards in section 122 of the Act. These safeguards relate to the copying, dissemination, retention of material obtained by equipment interference and are explained in Chapter 8 of this code.
- **The Secretary of State has consulted the Prime Minister** where the additional protection for Members of Parliament and other relevant legislatures applies (see section 106 of the Act).
- **Judicial commissioner approval.** Except in an urgent case, the issuing authority may not issue a warrant unless and until the decision to issue the warrant has been approved by a Judicial Commissioner. Section 103 of the Act sets out that the Judicial Commissioner must review the conclusions that have been reached as to whether the warrant is necessary on one or more of the grounds and whether the conduct that would be authorised is proportionate to what is sought to be achieved.

Authorisation of a targeted equipment interference warrant: senior officials and appropriate delegates

4.36 When it is not reasonably practicable for the Secretary of State or law enforcement chief to sign an equipment interference warrant a delegate may sign the warrant on their behalf. Typically this scenario will arise where the appropriate Secretary of State or law enforcement chief is not physically available to sign the warrant because, for example, they are on a visit or, in the case of a Secretary of State, in their constituency. Where the warrant is required by a Security and Intelligence Agency, or Defence Intelligence, the Secretary of State or member of the Scottish Government must still personally authorise the equipment interference. When seeking authorisation the senior official must explain the case, either in writing or orally, to the Secretary of State and this explanation should include considerations of necessity and proportionality. Once authorisation has been granted the warrant may be signed by a senior official. If the Secretary of State refuses to authorise the warrant the warrant must not be issued. When a law enforcement chief is unable to sign and issue a warrant an appropriate delegate[16] may exercise the power to issue the warrant. When a warrant is issued in this way the warrant instrument must contain a statement to that effect. Except in urgent cases, the decision to issue the warrant must then be approved by a Judicial Commissioner before the warrant is issued.

[16] Appropriate delegates are listed in Annex A.

Authorisation of equipment interference techniques for law enforcement agencies

4.37 Law enforcement chiefs may only issue an equipment interference warrant if they consider that it is proportionate for the warrant to be issued to their appropriate law enforcement officer. In addition to the factors set out in paragraph 4.35 above, in considering whether it is proportionate, the law enforcement chief should consider the full context of the application, including:

- Whether the appropriate law enforcement officer, or those effecting the warrant on his behalf, have the capabilities to conduct the equipment interference techniques sought under the warrant;
- Whether the equipment interference technique that is sought under the warrant been adequately tested for the proposed use;
- Whether the appropriate law enforcement officer, or those effecting the warrant on his behalf, have sufficient training and experience in conducting the equipment interference techniques sought under the warrant;
- If the equipment interference technique is sensitive, whether there are sufficient safeguards in place to ensure that the technique is protected; and
- Whether it would be more proportionate for another law enforcement agency to obtain the warrant on their behalf.

4.38 The Secretary of State may issue further guidance to assist law enforcement chiefs in considering whether it is proportionate to issue a warrant to their appropriate law enforcement officer. These considerations will ensure that equipment interference techniques are deployed by law enforcement agencies in a consistent and proportionate manner.

4.39 Some law enforcement agencies may only carry out equipment interference for the purpose of preventing or detecting serious crime when also in relation to specific functions of their agency. These are:

- For immigration officers, the serious crime must relate to an offence which is an immigration or nationality offence;
- For Revenue and Customs, the serious crime must relate to an assigned matter within the meaning of section 1(1) of the Customs and Excise Management Act 1979;
- For a designated customs official, the serious crime must relate to a matter in respect of which a designated customs official has functions; and,
- For the Competition and Markets Authority, the serious crime must relate to offences under section 188 of the Enterprise Act 2002.

Collateral intrusion

4.40 Before authorising applications for equipment interference warrants, the person issuing the warrant should also take into account the risk of obtaining communications, equipment data or other information about persons who are not the targets of the equipment interference activity (collateral intrusion). Particular consideration should be given in cases where religious, medical, journalistic or legally privileged material may be involved, or where communications between a Member of Parliament[17] and another person on constituency business may be involved.

4.41 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 targeted 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. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the equipment interference activity.

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

Example: An equipment interference agency seeks to conduct equipment interference against a device used by a subject, T, on the grounds that this is necessary and proportionate for a relevant statutory purpose. It is assessed that the operation will unavoidably result in the obtaining of some information about members of T's family, who are also users of his device, and who are not the intended subjects of the equipment interference. The person issuing the warrant should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the authorisation. This may include minimising the obtaining of any material clearly relating to T's family and in the event it is inadvertently captured, applying the safeguards in the Act, including destroying material which is no longer relevant.

4.43 Where it is proposed to conduct equipment 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 equipment interference activity should be carefully considered against the necessity and proportionality criteria.

Example: An equipment interference agency seeks to establish the whereabouts of N. It is proposed to conduct equipment interference against P, who is an associate of N but who is not assessed to be of direct intelligence concern. The equipment interference will enable surveillance to be conducted via P's device, in order to obtain information about N's location. In this situation, P will be the subject of the equipment interference warrant and the person issuing the warrant should consider the necessity and proportionality of conducting surveillance against P, bearing in mind the availability of any other less intrusive means to identify N's whereabouts. It may be the case that the surveillance conducted via P's device will also result in obtaining information about P's family, which in this instance would represent collateral intrusion also to be considered by the person issuing the warrant.

[17] References to a Member of Parliament include references to a member of the House of Commons, the House of Lords, a UK member of the European Parliament, and members of the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

Power of Scottish Ministers to issue warrants

4.44 Equipment interference warrants may be issued on "serious crime" grounds by Scottish ministers, by virtue of arrangements under the Scotland Act 1998. The functions of the Scottish ministers also cover renewal, modification and cancellation arrangements. Sections 98 of the Act makes provision for Scottish Ministers to issue targeted equipment interference warrants for serious crime purposes in certain circumstances. Scottish Ministers may issue a targeted examination warrant for serious crime purposes providing the warrant, if issued, would relate only to a person that would be in Scotland at the time of the issue of the warrant or whom the Secretary of State believes would be in Scotland at that time.

Judicial commissioner approval

4.45 Before a targeted equipment interference warrant comes into force, its issuance must be approved by a Judicial Commissioner. Section 103 of the Act sets out the test that a Judicial Commissioner must apply when deciding whether to approve the issuance of an equipment interference warrant. This includes reviewing the warrant issuer's conclusion on whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved.

4.46 In reviewing these factors, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review, while ensuring compliance with the general duties in relation to privacy imposed by section 2 of the Act. The Judicial Commissioner may seek clarification from the warrant granting department or warrant seeking agency as part of their considerations.

4.47 If the Judicial Commissioner refuses to approve the decision to issue a warrant the warrant issuer may either:

- not issue the warrant; or,
- refer the matter to the IPC for a decision (unless the IPC has made the original decision).

4.48 If the IPC refuses the decision to issue a warrant the warrant issuer must not issue the warrant. There is no further avenue of appeal available.

4.49 The Act does not mandate how the Judicial Commissioner must show or record their decision. These practical arrangements should be agreed between the relevant public authorities and the Investigatory Powers Commissioner. The Act does not, for example, require the Judicial Commissioner to sign a legal instrument. This means that a Judicial Commissioner can provide oral approval to issue a warrant. It is important that a written record is taken of any such approvals.

Urgent authorisation of a targeted equipment interference warrant

4.50 The Act makes provision for cases in which a targeted equipment interference warrant is required urgently.

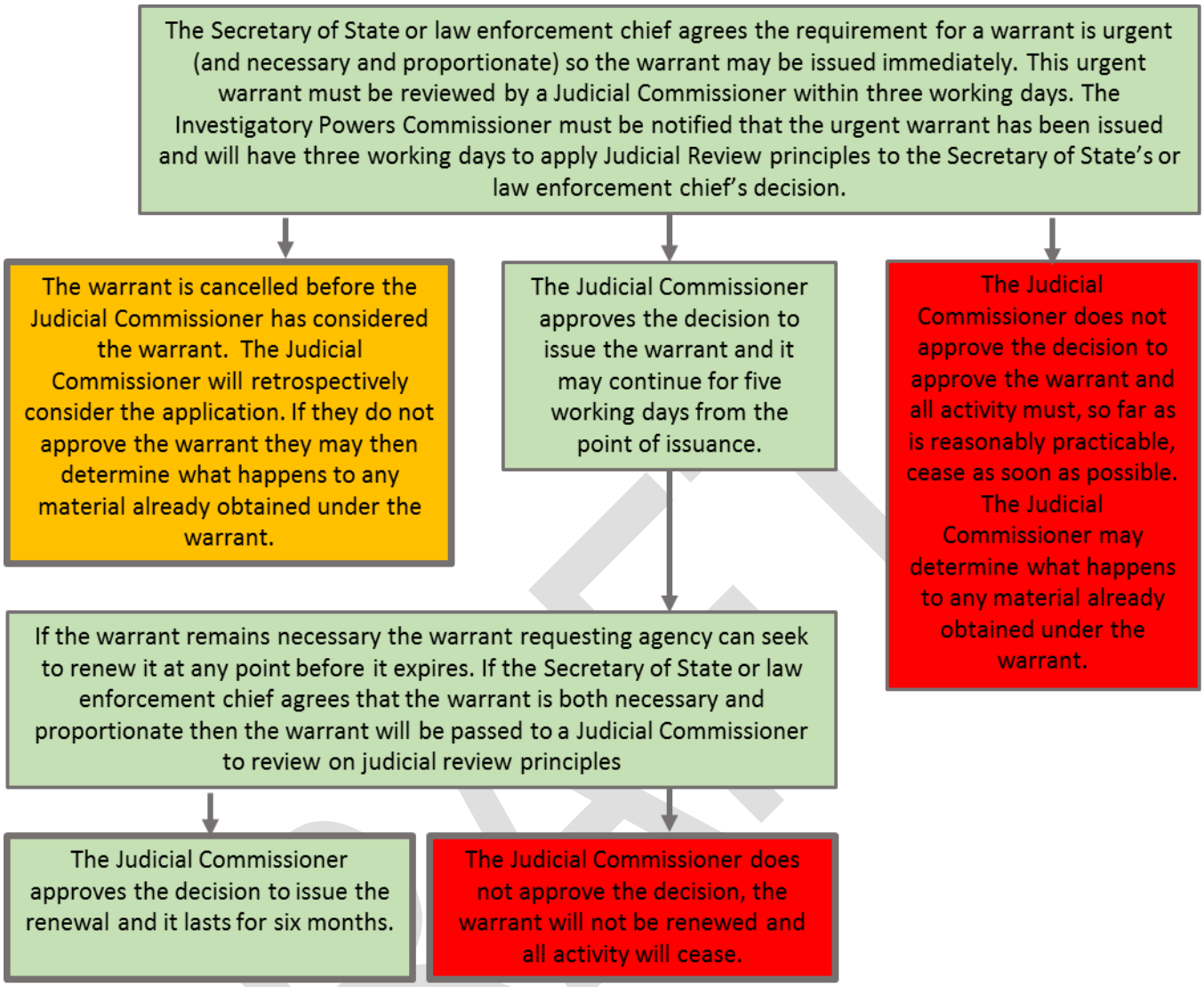
4.51 What constitutes an urgent case is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the requisite time. The requisite time reflects when the authorisation needs to be in place to meet an operational or investigative need. Urgent warrants should fall into at least one of the following three categories:

- Imminent threat to life or serious harm - for example, if an individual has been kidnapped and it is assessed that his life is in imminent danger;
- An intelligence gathering opportunity which is significant because of the nature of the potential intelligence, the operational need for the intelligence is significant, or the opportunity to gain the intelligence is rare or fleeting – for example, a group of terrorists is about to meet to make final preparations to travel overseas;
- A significant investigative opportunity - for example, a consignment of Class A drugs is about to enter the UK and law enforcement agencies want to have coverage of the perpetrators of serious crime in order to effect arrests.

4.52 The decision by the issuing authority to issue an urgent warrant must be reviewed by a Judicial Commissioner within three working days following the day of issue. In the case of warrants signed by a senior official the Judicial Commissioner's review should be on the basis of a written record, including any contemporaneous notes, of any oral briefing (and any questioning or points raised by the Secretary of State) of the Secretary of State by a senior official, or of the decision taken by the appropriate delegate to a law enforcement chief.

4.53 If the Judicial Commissioner retrospectively agrees to the Secretary of State's, law enforcement chief's or appropriate delegate's issuance of the urgent warrant, and it is still considered necessary and proportionate by the warrant requesting agency, renewal of the urgent warrant may be sought. A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed. If it is renewed it expires after six months, in the same way as non-urgent targeted equipment interference warrants. It is acceptable for the Secretary of State to decide to renew an urgent warrant. In these circumstances, the application to approve the urgent warrant can be presented to the Judicial Commissioner at the same time as they are considering the Secretary of State's decision to renew the warrant.

4.54 The following diagram illustrates the urgent authorisation process:



Warrants ceasing to have effect and retrieval of equipment

4.55 Where a Judicial Commissioner refuses to approve a decision to issue an urgent equipment interference warrant, the equipment interference agency must, as far as reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

4.56 The equipment interference agency may make representations to the Judicial Commissioner about the following matters:

- Whether further equipment interference should be authorised to enable the agency to secure that anything in the process of being done under the warrant stops as soon as possible;
- destruction of any material obtained under the warrant; and
- the conditions that should be imposed as to the use or retention of any of that material.

Format of equipment interference warrants

4.57 The warrant must describe the type of equipment that is to be interfered with and the conduct that the person to whom the warrant is addressed is authorised to take. The warrant must include the details specified in the second column of the Table in section 108 of the Act that relate to relevant equipment described in the first column.

4.58 Each warrant will comprise a warrant instrument signed by the person responsible for issuing the warrant and may also include a schedule or set of schedules. The warrant instrument will include:

- A statement that it is a targeted equipment interference warrant;
- The subject of the equipment interference to which the warrant relates[18]. Where required, descriptions on the instrument can be in the form of an alias or other description that identifies the subject;
- A warrant reference number; and
- The persons who may subsequently modify the warrant in an urgent case (if authorised in accordance with section 112 of the Act).

4.59 An equipment interference warrant may expressly authorise the disclosure of any material obtained under the warrant. However, a warrant does not need to specify all potential disclosures of material. Disclosure of material is permitted provided that it is not an unauthorised disclosure for the purposes of section 124 of the Act. This may include, for example, disclosure of material for admission as evidence in criminal and civil proceedings.

Duration of equipment interference warrants

4.60 Targeted equipment interference warrants and targeted examination warrants issued using the standard procedure are valid for an initial period of six months. Warrants issued under the urgency procedure are valid for five working days following the date of issue unless renewed by the issuing authority.

4.61 Upon renewal, warrants are valid for a further period of six months. This period begins on the day after the day on which the warrant would have expired, had it not been renewed. In practice this means that if a warrant is due to end on 3 March but is renewed on 1 March, the renewal takes effect from 4 March and the renewed warrant will expire on 3 September. An equipment interference warrant may only be renewed in the last 30 days of the period for which it has effect.

4.62 Where a combined equipment interference warrant includes warrants or authorisations which would cease to have effect at the end of different periods, the combined warrant will expire at the end of the shortest of the periods.

4.63 Where modifications to an equipment interference warrant are made, the warrant expiry date remains unchanged. However, where the modification takes place under the urgency provisions, the modification expires after five working days following the date of issue, unless it is renewed in line with the routine procedure.

4.64 Where a change in circumstance leads the equipment interference agency to consider it no longer necessary, proportionate or practicable for a warrant to be in force, the agency must make a recommendation to the issuing authority that it should be cancelled with immediate effect.

[18] Eligible subject-matters of equipment interference warrants are set out in section 101.

Modification of a targeted equipment interference warrant

4.65 Equipment interference warrants may be modified under the provisions of sections 111 and 116 of the Act. The modifications that may be made are:

- adding to the matters to which the warrant relates;
- removing a matter to which the warrant relates;
- adding any name or description to the names or descriptions included in the warrant. Such a modification cannot be made to a warrant which relates to a targeted subject i.e. that relates to a particular person, organisation or location;
- varying or removing any such name or description. Such a modification cannot be made to a warrant which relates to a targeted subject i.e. that relates to a particular person, organisation or location;
- adding to the descriptions of types of equipment;
- varying or removing a description of a type of equipment.

4.66 The modifications above may be made providing that the conduct authorised by the modification is within the scope of the original warrant. It is for this reason that section 111(3) prohibits modifications to add, vary or remove the name or descriptions of a targeted warrant that relates to just one specified person, organisation or location, as such a modification would go beyond the original scope of the targeted warrant. In practice this means that a warrant which relates to a targeted subject cannot be modified into a targeted thematic warrant; a fresh warrant would be required. Modifications to add names or descriptions, which fall within the scope of the original warrant, are required to be made to targeted thematic warrants when it is reasonably practicable to do so (see para 4.25).

4.67 Three examples are provided below – the first would not be permitted, but the second and third would be:

Example of a modification that would not be permitted:
An equipment interference agency obtains a targeted equipment interference warrant relating to equipment associated with a specific serious criminal known as 'Mr. Big'. The issuing authority, with Judicial Commissioner approval, issues the warrant authorising the interference of equipment of 'Mr. Big'. The investigation progresses and the equipment interference agency wants to interfere with the equipment of one of 'Mr. Big's' associates. This would require a new warrant – the warrant against 'Mr. Big' cannot be modified so it is against an additional person.

Example of a modification that would be permitted:
An equipment interference agency obtains a targeted thematic equipment interference warrant relating to equipment associated with a specific serious criminal known as 'Mr. Big' and his unidentified associates. The issuing authority, with Judicial Commissioner approval, issues the warrant authorising the interference of equipment of "'Mr. Big' and his unidentified associates investigated under Operation NAME". The investigation progresses and the equipment interference agency wants to interfere with the equipment of one of 'Mr. Big's' associates. The warrant could be modified to add the name or description of the associate, if reasonably practicable to do so, and the associate's equipment if it did not fall within the type of equipment already described on the warrant.

Example of a modification to add a new subject matter but still stay within the scope of the original warrant: An equipment interference agency obtains a targeted thematic equipment interference warrant relating to equipment associated with a specific malware attack against UK critical national infrastructure. Initially the subject matter of the warrant is defined as clause 96(1)(e) – equipment in more than one location, where the interference is for the purpose of a single investigation or operation. Data obtained indicates that the same equipment is being used for stealing high financial value commercial secrets from a financial institution. In order to investigate the secondary activity, the warrant could be modified to include a new subject matter clause 96(1)(b) – equipment belonging to, used by, or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity. The same devices are targeted and the same conduct is used to obtain the data for both the malware attack and the theft, so the scope of the warrant stays the same.

4.68 A modification may be made by the following persons in circumstances where the person considers that the modification is necessary on any relevant grounds:

- The Secretary of State, in the case of a warrant issued by the Secretary of State;
- A member of the Scottish Government, in the case of a warrant issued by the Scottish Ministers
- A senior official acting on behalf of the Secretary of State or (as the case may be) the Scottish Ministers, or
- A law enforcement chief or the chief's appropriate delegate, in the case of a warrant issued by a law enforcement chief or the chief's appropriate delegate.

4.69 As soon as is reasonably practicable after a person makes a modification to a warrant, a Judicial Commissioner must be notified of the modification and the reason for making it. This does not apply if:

- the modification is an urgent modification (where different notification provisions are provided for, detailed below at Paragraph 4.71),
- sections 106 or 107 apply, or
- the modification is to remove any matter, name or descriptions included in the warrant in accordance with section 108 (3) to (5).

4.70 In the case of a modification of a warrant issued to a law enforcement officer, the decision to make a modification must be approved by a Judicial Commissioner. This ensures that independent consideration is applied to applications for modifications. In the case of a modification of a warrant issued to a security and intelligence agency or Ministry of Defence, the decision to approve a modification can be made by a senior official in the warrant granting department. Where a modification of a warrant is made by a senior official, the Secretary of State or (in the case of a warrant issued by the Scottish Minister) a member of the Scottish Government must be notified personally of the modification and the reasons for making it.

Administrative clarifications of targeted warrants

4.71 Sections 111(5) and 116(11) clarify that a modification is only required where the conduct authorised by the warrant is affected. For example, where more detail is provided for clarification, such as the full name of a person as it becomes known rather than an alias, the administrative clarification will be covered by sections 111(5) and 116(11) as long as the subject of the equipment interference is still accurately described (i.e. there is not a change in the scope of the equipment interference). Similarly, an equipment interference agency may wish to update the subject matter of a thematic warrant from time to time without modifying the scope of the conduct authorised, or the equipment to be interfered with, in which case the modification will fall within this provision. Nonetheless, equipment interference agencies should take measures to keep warrant granting departments up to date with any new information.

Example: An equipment interference agency obtains a warrant against equipment used by a criminal front company to facilitate serious crime. This company regularly changes the name it trades under but the criminal activity behind it and the equipment used remains constant. There is no change in the scope of the warrant but the granting department is kept up to date periodically with the list of names used by the company.

Urgent modification of targeted warrants

4.72 Sections 115 and 117 of the Act make provision for cases in which modifications of a targeted warrant are required urgently. A modification will only be considered urgent if there is a very limited window of opportunity to act. For example, this may include a threat to life situation, where a kidnap has taken place, in the immediate aftermath of a major terrorist incident or where intelligence has been received that a significant quantity of drugs is about to enter the country. In some cases, the modification will necessarily be short-lived, for instance if a kidnap is quickly resolve.

4.73 For the Security and Intelligence Agencies, a senior official in the equipment interference agency may make the urgent modification but it must be approved by a senior official in the warrant granting department within five working days. A judicial commissioner must be notified as soon as is reasonably practicable after the senior official in the warrant granting department makes a decision and the Secretary of State or member of Scottish Government will also be notified personally. In the event that the warrant granting department does not agree to the urgent modification, the activity conducted under the urgent modification up to that point remains lawful. The senior official in the warrant granting department may authorise further interference, but only in the interest of ensuring that anything being done is stopped as soon as possible. The Secretary of State should be informed of any additional interference that has been authorised.

4.74 In the case of law enforcement agencies, the relevant law enforcement chief or an appropriate delegate may make the urgent modification. The modification then must be considered by a judicial commissioner within five working days. In the event that the judicial commissioner does not agree to the urgent modification, the activity conducted under the urgent modification remains lawful. If the judicial commissioner refuses to approve the decision to make a modification they may authorise further interference, but only in the interest of ensuring that anything being done by virtue of the modification is stopped as soon as possible.

Renewal of a targeted equipment interference warrant

4.75 Section 110 of the Act sets out that the appropriate person may renew a warrant at any point before its expiry date. Applications for renewals of warrants should contain an update of the matters outlined in paragraph 4.10 above. In particular, the applicant should give an assessment of the value of equipment interference to date and explain why it is considered that equipment interference continues to be necessary for one or more of the relevant grounds, and why it is considered that the interference continues to be proportionate. Consideration of the extent (if any) of collateral intrusion that has occurred to date, and how this has been managed, will be relevant to the consideration of proportionality. Sections 106 (additional protection for Members of Parliament) and 107 (items subject to legal professional privilege) apply in relation to the renewal of warrants in the same way as they apply to a decision to issue a warrant.

4.76 In all cases, a warrant may only be renewed if the renewal has been approved by a Judicial Commissioner. An equipment interference warrant may only be renewed in the last 30 days of the period for which it has effect.

4.77 A copy of the warrant renewal instrument will be forwarded to all persons on whom a copy of the original warrant has been served, providing they are still actively assisting with the implementation of the warrant. A warrant renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

Warrant cancellation

4.78 Any of the persons authorised to issue warrants under Part 5 may cancel a warrant at any time. If an appropriate person[19] within the issuing authority considers that such a warrant is no longer necessary or that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct, the appropriate person must cancel the warrant. Equipment interference agencies therefore will need to keep their warrants under review and must notify the issuing authority if the equipment interference agency assess that the warrant is no longer necessary or proportionate. In practice, in the case of the Security and Intelligence Agencies and Defence Intelligence, the responsibility to cancel a warrant will be normally exercised by a senior official in the warrant granting department on behalf of the Secretary of State. The equipment interference agency should take steps to cease the interference as quickly as possible if they consider that the warrant is no longer necessary or proportionate – they should not wait until the necessary cancellation instrument has been signed.

4.79 The Act requires the person to whom a warrant is addressed to ensure that anything in the process of being done under the warrant stops as soon as possible, so far as is reasonably practicable. In some circumstances it may be impossible, or not reasonably practicable, to cease all elements of interference upon cancellation of a warrant. In deciding what ought to be done to achieve this, an equipment interference agency must consider what further interference with equipment and privacy might be necessary and whether it is proportionate to undertake it (without further authorisation) in order to stop the original activity. In cases of doubt equipment interference agencies may seek advice from the IPC.

[19] Section 118 (4) define ‘appropriate persons’

4.80 The cancellation instrument should be addressed to the person to whom the warrant was issued and should include the reference number of the warrant and the description of the equipment specified in the warrant. A copy of the cancellation instrument should be sent to any persons who have assisted in giving effect to the warrant in the preceding twelve months.

Combined warrants

4.81 Where an equipment interference agency wishes to conduct equipment interference but not all of the proposed conduct can properly be authorised under an equipment interference warrant, additional warrants or authorisations will be required. The agency may either obtain a combined warrant or may obtain separate warrants/authorisations pursuant to the Act and RIPA, the 1997 Act and/or the 1994 Act.

Example: An equipment interference agency wishes to covertly enter residential premises to search for physical evidence and also download material from a device located within the premises. The obtaining of material from the device constitutes equipment interference. However, the associated trespass to property is a separate interference with property and the intrusive surveillance is not linked to the communications, equipment data or other information obtained from the equipment interference. The trespass to property and intrusive surveillance cannot be authorised by the equipment interference warrant and must be authorised by a property interference authorisation and intrusive surveillance authorisation respectively. All three authorisations relate to the same operational activity and the same information will be relevant across the applications. A combined warrant is therefore likely to be appropriate.

4.82 Schedule 8 to the Act provides for combined warrants. Combining warrant applications is not mandatory, but provides the option for grouping warrant applications for the same operational activity together so that the full range of actions that may be undertaken can be addressed. This allows issuing authority and/or Judicial Commissioner to consider the full range of actions that may be undertaken in relation to the investigation. In appropriate cases, it can allow a more informed decision about the necessity and proportionality of the totality of the action to be authorised and can also be more efficient for the agency applying for the warrant.

4.83 For combinations of warrants under schedule 8, the authorisation process set out at paragraph 4.35 onwards will apply. In some cases this will necessitate a higher authorisation process than would otherwise be required for individual warrant applications. Where two warrants are combined that would otherwise be issued by different authorities (for example, an equipment interference warrant issued by a law enforcement chief and an interception warrant issued by a Secretary of State), the warrant will always be issued by the higher authority level. Where part of a combined warrant is cancelled, the whole warrant ceases to have effect under the same procedures set out at paragraph 4.78.

4.84 Where warrants are sought urgently and the intention is to later proceed with a combined warrant application, such an application must be made before the urgent warrant authorisation ceases to have effect.

4.85 Per paragraph 20(1)(a) of Schedule 8, the duties imposed by clause 2 (having regard to privacy) apply to combined warrants as appropriate, e.g. when issuing, renewing or cancelling a Part 2, 5, 6 or 7 warrant, modifications, granting/approving or giving/varying/revoking notices. So the targeted equipment interference element of a combined warrant cannot be issued without having regard to privacy per clause 2.

4.86 The exclusion of matters from legal proceedings (section 53) continues to apply to an interception warrant that is part of a combined warrant. However, when an equipment interference warrant is combined with an interception warrant the material derived from equipment interference may still be used in legal proceedings if required. If material derived from equipment interference authorised by a combined warrant can be recognised as a product of interception, and therefore reveals the existence of a warrant issued under Chapter 1 of Part 1 of the Act, the material is excluded from use in legal proceedings according to section 53 of the Act.

4.87 Should the exclusion from legal proceedings mean that there may be difficulties in disclosing any material obtained under a combined warrant that included an interception warrant, equipment interference agencies may wish to consider the possibility of seeking individual warrants instead.

Applications made by or on behalf of the Security and Intelligence Agencies

4.88 Paragraph 1 of Schedule 8 sets out that the Secretary of State may issue a warrant that combines a targeted interception warrant with a targeted equipment interference warrant issued under section 19. Such warrants will only be available to agencies that can apply for equipment interference warrants and interception warrants. Paragraph 8 of Schedule 8 sets out that the Secretary of State may also combine a targeted equipment interference warrant under section 97 with one or more of the following:

- A targeted examination warrant under section 1(2) or section 97(3)
- A directed surveillance authorisation under section 2 of RIPA
- An intrusive surveillance authorisation under section 2 of RIPA
- A property interference authorisation under section 5 of the Intelligence Services 1994

4.89 Paragraph 4 sets out that a Scottish Minister may issue a warrant combining a targeted equipment interference warrant under section 98(1) with a targeted interception warrant under and/or a targeted examination warrant under section 21.

4.90 Paragraph 8 of Schedule 8 sets out that the Secretary of State may issue a warrant that combines a targeted equipment interference warrant with one or more of the following:

- A targeted examination warrant under section 97(3)
- A directed surveillance authorisation under section 2 of RIPA
- An intrusive surveillance authorisation under section 2 of RIPA
- A property interference authorisation under section 5 of the Intelligence Services Act 1994

Example: A security and intelligence agency wishes to conduct an operation which involves intrusive surveillance (provided for under section 5 of the Intelligence Services Act) and targeted equipment interference. Under Schedule 8 they may wish to combine these applications, so that the combined warrant is issued by the Secretary of State. In approving the decision to issue the warrant, the Judicial Commissioner would only consider the application for targeted equipment interference. Intrusive surveillance under section 5 of the 1994 Act cannot be combined with warrants outside of the Act e.g. Directed Surveillance Authorisations under Part 2 of RIPA.

Applications made by or on behalf of the Chief of the Defence Intelligence

4.91 Paragraph 9 of Schedule 8 sets out that the Secretary of State may, on an application made by or on behalf of the Chief of Defence Intelligence, issue a warrant that combines a targeted interception warrant with a targeted equipment interference warrant.

Applications made by or on behalf of a relevant law enforcement agency

4.92 Paragraph 11 of Schedule 8 sets out that the law enforcement chief may issue a warrant that combines a targeted equipment interference warrant with one or more of the following:

- A directed surveillance authorisation under section 2 of RIPA
- An intrusive surveillance authorisation under section 2 of RIPA
- A property interference authorisation under the 1997 Act

Example 1: An equipment interference agency wishes to conduct equipment interference to acquire private information from a computer and intercept an online video call in the course of its transmission. This activity constitutes both equipment interference and live interception. The interception cannot be authorised as incidental conduct so a combined interception and equipment interference warrant must be obtained. The combined warrant will be issued by the Secretary of State and approved by a Judicial Commissioner.

Example 2: An equipment interference agency wishes to conduct an operation which involves directed surveillance (provided for under Part 2 of RIPA) and targeted equipment interference. Under Schedule 8 they may wish to combine these applications. For a warrant issued to the head of an intelligence service the combined warrant would be issued by the Secretary of State and approved by a Judicial Commissioner. For a law enforcement agency, the relevant law enforcement chief would consider the directed surveillance activity as part of the entire combined applications. This entire combined application would also require approval by a Judicial Commissioner.

4.93 The above considerations do not preclude equipment interference agencies from obtaining separate warrants where appropriate. This may be required in order to preserve sensitive techniques, or may be more efficient if other authorisations are already in place.

Example: An equipment interference agency is monitoring a subject under the authority of a directed surveillance authorisation. An opportunity is identified to conduct equipment interference on the subject's device. It is necessary to continue to monitor the subject to ensure the equipment interference can be conducted covertly and to minimise the risk of compromise. Provided this continued surveillance is authorised under the existing directed surveillance authorisation, a further surveillance authorisation would not be required and therefore a combined warrant is not likely to be appropriate and a separate equipment interference authorisation could be obtained.

Collaborative working

4.94 Any person applying for an equipment interference warrant will need to be aware of particular sensitivities in the local community where the interference is taking place which could impact on the deployment of equipment interference capabilities. Equipment interference agencies must also take reasonable steps to de-conflict (as relevant) with other relevant services or law enforcement agencies. Where a warrant applicant considers that conflicts might arise with another equipment interference agency, they should consult a senior colleague within the other agency.

4.95 In cases where one equipment interference agency is acting on behalf of another, the tasking agency should normally obtain the equipment interference warrant. For example, where equipment interference is carried out by a police force in support of NCA, the warrant would usually be sought by the NCA. Where the operational support of other agencies (in this example, the police) is foreseen, this should be reflected in the warrant application and specified in the warrant. However, where an equipment interference agency considers it would be more proportionate for another agency to obtain the warrant on their behalf that other agency must obtain the equipment interference warrant. For example, where a police force considers that there are not sufficient safeguards in place to ensure the protection of a sensitive technique, it may approach the NCA to obtain the warrant.

4.96 Where possible, equipment interference agencies should seek to avoid duplication of warrants as part of a single investigation or operation. For example, where two police forces are conducting equipment interference as part of a joint operation, only one warrant is required. Duplication of warrants does not affect the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on agencies.

4.97 Where an individual or a non-governmental organisation is acting under direction of an equipment interference agency any activities they conduct which comprise equipment interference for the purposes of the Act definitions, should be considered for authorisation under that Act.

4.98 There are two further important considerations with regard to collaborative working:

- Applications for equipment interference warrants by police forces must only be made by a member or officer of the same force as the law enforcement chief, unless the chief officers of the forces in question have made a collaboration agreement under the Police Act 1996 and the collaboration agreement permits applicants and law enforcement chiefs to be from different forces.
- Applications for equipment interference warrants by law enforcement agencies other than police forces must only be made by a member or officer of the same force or agency as the law enforcement chief regardless of which force or agency is to conduct the activity.

4.99 Without limiting the ability of equipment interference agencies to work collaboratively, as out lined above, applications for equipment interference warrants may only be issued to a member of the same equipment interference agency as made the application, except where specified law enforcement agencies have entered into a relevant collaboration agreement under the Police Act 1996 which permits this rule to be varied.

4.100 This exception only applies to police forces and the National Crime Agency, where they are able to enter into collaboration agreements under the Police Act 1996. The collaboration agreement must permit the law enforcement chief of one collaborating law enforcement agency to issue a warrant to an applicant from another collaborating law enforcement agency.

4.101 Where, pursuant to a collaboration agreement, the Director General of the National Crime Agency is the law enforcement chief for an application made by a member of a collaborative police force, the Director General may only issue the warrant if he considers there is a British Islands connection. This reflects the general restriction that warrants should only be issued to police forces where there is a British Islands Connection (see further at paragraph 2.33).

4.102 When collaboration between equipment interference agencies is expected to be required for an operation from the outset the warrant applicant must name each agency in the warrant application. The application should set out why the involvement of each additional agency is required and to what extent they are intended to be involved in the proposed equipment interference. The warrant application should describe specifically the equipment interference that each individual agency is required to conduct.

4.103 Any equipment interference warrant that specifically authorises the activity of multiple equipment interference agencies should specify any relevant restrictions on the sharing of information derived from the interference between such agencies.

4.104 Where an equipment interference agency requires an international partner– who is not therefore an equipment interference agency as defined by the Act – to undertake an action authorised by an equipment interference warrant, this must be clearly specified within the warrant application. The application must make clear why the assistance of an international partner is required and specify the activity that the equipment interference agency intends to request of that partner. Once a warrant is issued, an equipment interference agency may work collaboratively with an international partner to carry out equipment interference in accordance with that warrant by virtue of section 94 (5) (b) of the Act.

5 Bulk equipment interference warrants

5.1 This Chapter provides guidance on bulk equipment interference warrants issued under Chapter 3 of Part 6 of the Act and the safeguards that apply to the selection for examination of material obtained under such a warrant. Bulk equipment interference warrants and targeted examination warrants may only be issued to the Security and Intelligence Agencies.

5.2 The safeguards that apply to the access, retention, disclosure, deletion and destruction of all communications, information and equipment data obtained under targeted and bulk equipment interference warrants are set out in Chapter 8 of the code.

Bulk equipment interference

5.3 Bulk equipment interference warrants are described in section 163 of the Act. Under bulk warrants, the subsequent examination of any material collected under the warrant is controlled by additional statutory access controls (e.g. operational purposes, necessity and proportionality tests). Further safeguards are applied to the examination of communications and private information of individuals within the British Islands – a separate targeted examination warrant, subject to the full "double-lock" authorisation process, is required to examine this material.

5.4 Bulk warrants will usually only be appropriate for large scale operations, and are only available for operations for the obtaining of overseas related communications, overseas-related information or overseas-related equipment data.

5.5 To determine whether a thematic or bulk warrant is appropriate, regard must be given in particular to whether the Secretary of State is able to foresee the extent of all of the interferences to a sufficient degree to properly and fully assess necessity and proportionality *at the time of issuing the warrant*. This includes consideration of interferences in relation to all those individuals affected, whether the intended target of the interference or those affected incidentally. Where this can be done, usually due to the specific identity of the target being known in advance or a specific identifier relating to the target individuals' communications or devices, a thematic warrant is likely to be most appropriate. This is because the additional access controls of the bulk regime are not required if a greater degree of targeting, or the filtering or processing of data at or soon after the point of collection, can limit interference such that the Secretary of State and the Judicial Commissioner can adequately address all of those considerations (e.g. necessity and proportionality, purpose, protection for UK persons' content) from the outset. Based on the scenario given at 4.34, the following example demonstrates the difference between thematic and bulk equipment interference:

Example: Intelligence suggests that a Daesh-inspired cell in a particular location in the Middle East is plotting an imminent bomb attack against UK interests in the region. Little is known about the individual members of the terrorist cell. However, it is known that a particular software package is commonly – but not exclusively – used by some terrorist groups. After using equipment interference to obtain equipment data from a large number of devices in the specified location, analysts apply analytical techniques to the data, starting with a search term ('selector') related to the known software package, to find common factors that indicate a terrorist connection. A series of refined searches of this kind, using evolving factors that are uncovered during the course of the analytical process, gradually identify devices within the original 'pot' of data collected that belong to the terrorist cell. Their communications (including content) can then be retrieved and examined.

As the cell members can only be identified through a series of refined searches that cannot all be assessed in advance at the time the warrant is issued, second stage access controls are required to govern all of the data selection within the operation. Accordingly, a bulk equipment interference warrant is suitable.

Application for a bulk equipment interference warrant

5.6 An application for a bulk equipment interference warrant is made to the Secretary of State. As set out at section 165 of the Act, bulk equipment interference warrants are only available to the Security and Intelligence Agencies. An application for a bulk equipment interference warrant therefore may only be made by or on behalf of the following persons:

- The Director General of the Security Service;
- The Chief of SIS;
- The Director of GCHQ.

5.7 Bulk equipment interference warrants, when issued, are addressed to the head of the security and intelligence agency by whom, or on whose behalf, the application was made. A copy may then be served on any person who may be able to provide assistance in giving effect to that warrant. The purpose of such a warrant will typically reflect one or more of the intelligence priorities set by the National Security Council (NSC)[20].

5.8 Prior to submission, each application should be subject to a review within the agency making the application. This involves scrutiny by more than one official, who will consider whether the application is necessary for one or more of the permitted statutory purposes (in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security). One of the statutory purposes for which a bulk equipment interference warrant can be issued must always be national security. The scrutiny of the application will also include whether the equipment interference proposed is both necessary and proportionate and whether the examination of the material to be acquired is necessary for one or more of the operational purposes specified, and is proportionate in all the circumstances.

5.9 Each application, a copy of which must be retained by the applicant, should contain the following information:

- Background to the operation in question:
  - A general description of the equipment to be interfered with and the communications, information and equipment data to be obtained; and
  - Description of the conduct to be authorised, which must be restricted to the obtaining of overseas-related communications, overseas-related information or overseas-related equipment data, or the conduct (including the obtaining of other communications, information or equipment data not specifically identified by the warrant as set out at section 163(5)) that is necessary to undertake in order to carry out what is authorised or required by the warrant.

[20] One of the NSC's functions is to set the priorities for intelligence coverage for GCHQ and SIS.

- An assessment of the consequences (if any) and potential consequences of the conduct, including any risk of compromising the security of any equipment directly or indirectly involved with the interference and, in particular, whether this may enable further intrusion into privacy;
- The operational purposes for which the material obtained may be selected for examination and an explanation of why examination is necessary for those operational purposes proposed in the warrant;
- An explanation of why the equipment interference is considered to be necessary for one or more of the statutory purposes, which must always include an explanation of why the equipment interference is necessary in the interests of national security;
- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, explaining why less intrusive alternatives have not been or would not be as effective;
- An assurance that the material obtained will be selected for examination only so far as it is necessary for one or more of the operational purposes specified on the warrant and that it meets the other requirements of section 179 of the Act; and
- An assurance that all material will be kept for no longer than necessary and handled in accordance with the safeguards required by sections 177 of the Act.

Authorisation of a bulk equipment interference warrant

5.10 A bulk equipment interference warrant may only be issued if the Secretary of State considers that the purpose of the warrant is to obtain overseas-related communications, overseas-related information or overseas-related equipment data.

Necessity

5.11 The Secretary of State may only issue a bulk equipment interference warrant if the Secretary of State considers that the warrant is necessary in the interests of national security, or on that ground and for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the UK.

5.12 The power to issue a bulk equipment interference warrant for the purpose of safeguarding the economic well-being of the UK may only be exercised where it appears to the Secretary of State that the circumstances are relevant to the interests of national security. The Secretary of State will not issue a warrant on these grounds if a direct link between the economic well-being of the UK and national security is not established. Any application for a warrant for the purpose of safeguarding the economic well-being of the UK should therefore identify the circumstances that are relevant to the interests of national security.

5.13 As set out in section 165(3), the power to issue a bulk equipment interference warrant for the purpose of safeguarding the economic well-being of the UK may also only be exercised in circumstances where the information it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands.

5.14 Before issuing a bulk equipment interference warrant, the Secretary of State must also consider that the examination of material obtained under the warrant is necessary for one or more of the specified operational purposes (section 165(1)(d)). Material obtained under the warrant can only be selected for examination when necessary for one of the specified operational purposes. When considering the specified operational purposes, the Secretary of State must also be satisfied that any examination of the material obtained under the warrant for those purposes is necessary for one or more of the statutory purposes set out on the warrant (as at 165(1)(b) and 165(2) and (3)). For example, if a bulk equipment interference warrant is issued in the interests of national security and for the purpose of preventing or detecting serious crime, every specified operational purpose on that warrant must be necessary for one or both of these two broader purposes.

Proportionality

5.15 In addition to the consideration of necessity, the Secretary of State must be satisfied that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

5.16 In considering whether a bulk equipment interference warrant is necessary and proportionate, the Secretary of State must take into account whether what is sought to be achieved under the warrant could reasonably be achieved by other less intrusive means (section 2(2)(a) of the Act).

Safeguards

5.17 Before deciding to issue a warrant, the Secretary of State must consider that satisfactory arrangements are in force in relation to the warrant, setting out the safeguards for the copying, dissemination and retention of intercepted content and secondary data. These safeguards are explained in Chapter 8 of this code.

Authorisation of a bulk equipment interference warrant: senior officials

5.18 The Act permits that when it is not reasonably practicable for the Secretary of State to sign a bulk equipment interference warrant a delegate may sign the warrant on their behalf. Typically this scenario will arise where the appropriate Secretary of State is not physically available to sign the warrant because, for example, they are on a visit or in their constituency. The Secretary of State must still personally authorise the equipment interference. When seeking authorisation the senior official must explain the case, either in writing or orally, to the Secretary of State and this explanation should include considerations of necessity and proportionality. Once authorisation has been granted the warrant may be signed by a senior official. If the Secretary of State refuses to authorise the warrant the warrant must not be issued. When a warrant is issued in this way the warrant instrument must contain a statement to that effect. A warrant that has been signed by a senior official does not make it urgent unless there is a statement to that effect from the Secretary of State. Except in urgent cases the decision to issue the warrant must then be approved by a Judicial Commissioner before the warrant is issued.

5.19 The Act does not mandate how the Judicial Commissioner must show or record their decision. These practical arrangements should be agreed between the relevant public authorities and the Investigatory Powers Commissioner. The Act does not, for example, require the Judicial Commissioner to sign a legal instrument. This means that a Judicial Commissioner can provide oral approval to issue a warrant. It is important that a written record is taken of any such approvals.

Judicial Commissioner Approval

5.20 Following the decision to issue a bulk equipment interference warrant by the Secretary of State, it must be approved by a Judicial Commissioner.

5.21 Section 166 of the Act sets out the test that a Judicial Commissioner must apply when deciding whether to approve a bulk equipment interference warrant. The Commissioner must review the Secretary of State's conclusions as to

- whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved; and
- the necessity of examination for each of the specified operational purposes, including whether those operational purposes are necessary for the statutory purposes on the warrant.

5.22 In reviewing these factors, the Judicial Commissioner must apply judicial review principles to a sufficient degree to ensure compliance with the general duties in relation to privacy imposed by section 2 of the Act. The Judicial Commissioner may speak to the warrant granting department or warrant seeking agency as part of their considerations. If the Judicial Commissioner refuses to approve the decision to issue a warrant the Secretary of State may either:

- not issue the warrant;
- refer the matter to the IPC for a decision (unless the IPC has made the original decision).

5.23 If the IPC refuses the decision to issue a warrant the Secretary of State must not issue the warrant. There is no further avenue of appeal available to the Secretary of State.

Urgent authorisation of bulk equipment interference warrants

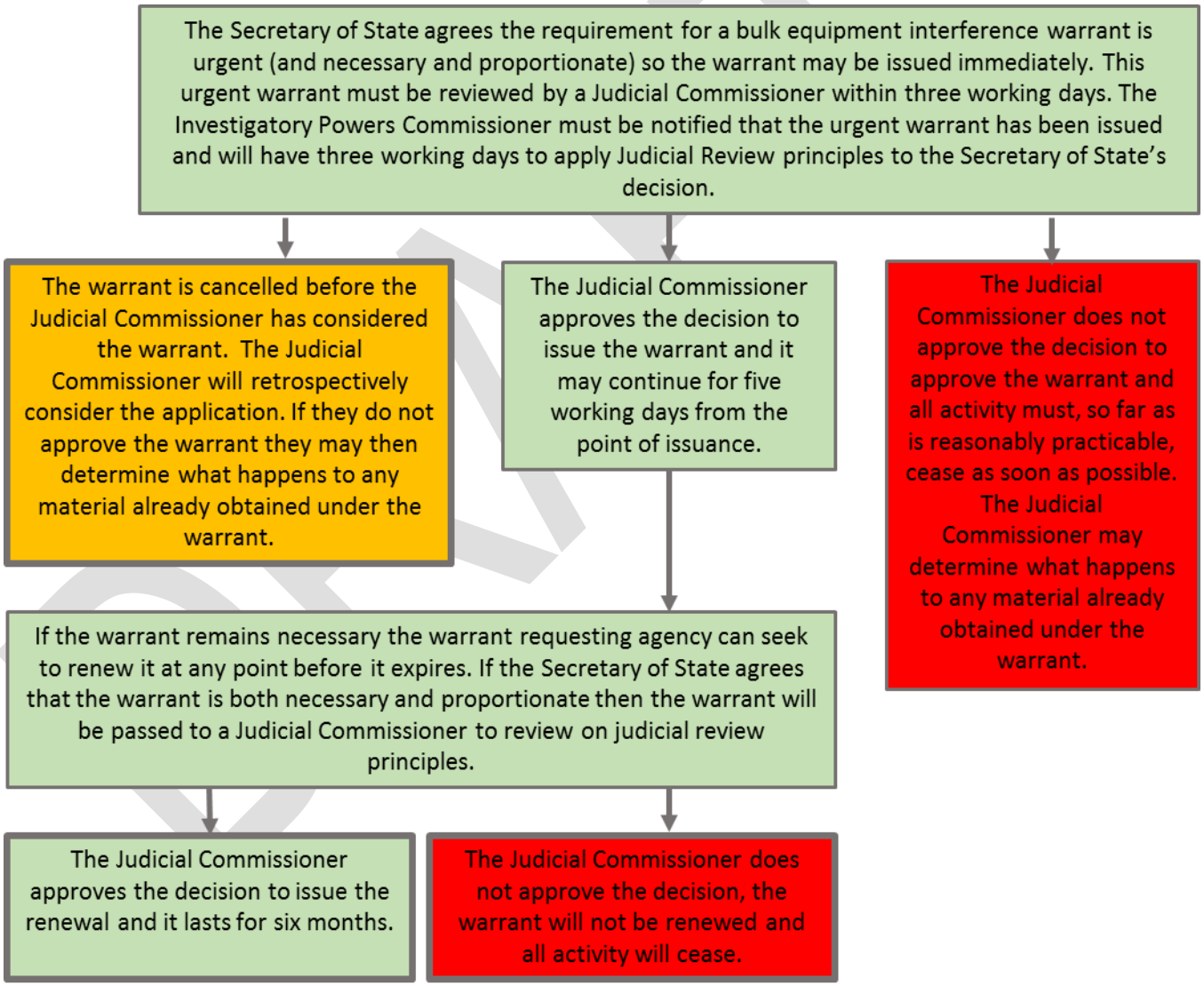
5.24 The Act makes provision for cases in which a bulk equipment interference warrant is required urgently. Urgency is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the requisite time. Accordingly, urgent warrants can permit equipment interference when issued by the issuing authority without prior approval from a Judicial Commissioner. The requisite time would reflect when the authorisation needs to be in place to meet an operational or investigative need. Urgent warrants should fall into at least one of the following three categories:

- Imminent threat to life or serious harm - for example, if there is intelligence to suggest an impending terrorist attack;
- An intelligence gathering opportunity which is significant because of the nature of the potential intelligence, the operational need for the intelligence is significant, or the opportunity to gain the intelligence is rare or fleeting – for example, a group of terrorists is about to meet to make final preparations to travel overseas;
- A significant investigative opportunity - for example, a consignment of weapons is about to enter the UK that the security and intelligence agencies eventually may be used for acts of terror.

5.25 The decision by the Secretary of State to issue an urgent warrant must be reviewed by a Judicial Commissioner within three working days following the day of issue. In the case of warrants signed by a senior official the Judicial Commissioner's review should be on the basis of a written record, including any contemporaneous notes, of any oral briefing (and any questioning or points raised by the Secretary of State) of the Secretary of State by a senior official.

5.26 If the Judicial Commissioner retrospectively agrees to the Secretary of State's issuance of the urgent warrant, and it is still considered necessary and proportionate by the warrant requesting agency, renewal of the urgent warrant may be sought. A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed. If it is renewed it expires after six months, in the same way as non-urgent targeted equipment interference warrants.

5.27 The following diagram illustrates the bulk equipment interference urgent authorisation process:



Warrants ceasing to have effect and retrieval of equipment

5.28 Where a Judicial Commissioner refuses to approve a decision to issue an urgent bulk equipment interference warrant, the equipment interference agency must, as far as reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

5.29 The equipment interference agency may make representations to the Judicial Commissioner about the following matters:

- Whether further equipment interference should be authorised to enable the agency to secure that anything in the process of being done under the warrant stops as soon as possible;
- destruction of any material obtained under the warrant; and
- the conditions that should be imposed as to the use or retention of any of that material.

Format of a bulk equipment interference warrant

5.30 A bulk equipment interference warrant must contain a provision stating that is a bulk equipment interference warrant. Each warrant is addressed to the head of the security and intelligence agency by whom, or on whose behalf, the application was made. Where relevant, a copy may then be served on any person who may be required to provide assistance in giving effect to the warrant. The warrant should include the following:

- A description of the conduct authorised by the warrant;
- The operational purposes for which any material obtained under the warrant may be selected for examination;
- The warrant reference number; and
- Details of the persons who may subsequently modify the operational purposes of a warrant in an urgent case.

Duration of bulk equipment interference warrants

5.31 Bulk equipment interference warrants issued using the standard procedure are valid for an initial period of six months. Warrants issued under the urgency procedure are valid for five working days following the date of issue unless renewed by the Secretary of State. Upon renewal, warrants are valid for a further period of six months. This period begins on the day after the day of which the warrant would have expired, had it not been renewed.

5.32 Where modifications to a bulk equipment interference warrant are made, the warrant expiry date remains unchanged. However, where the modification takes place under the urgency provisions, the modification instrument expires after five working days following the date of issue, unless it is renewed in line with the routine procedure.

Modification of a bulk equipment interference warrant

5.33 A bulk equipment interference warrant may be modified by an instrument under the provisions at section 173 of the Act. The modifications that can be made to a bulk equipment interference warrant are:

- to add, vary or remove an operational purpose specified on the warrant, for which material obtained under the warrant may be selected for examination; and
- to add to, vary or remove any part of the description of the conduct authorised by the warrant.

5.34 In circumstances where a modification is being made to add or vary an operational purpose or any part of the authorised interference, the modification must be made by a Secretary of State and must be approved by a Judicial Commissioner before the modification comes into force. The considerations set out in paragraphs 5.11 - 5.16 apply to a modification as they do to the issuing of a new warrant.

5.35 In circumstances where a bulk equipment interference warrant is being modified to remove an operational purpose or any part of the authorised interference, the modification may be made by the Secretary of State or by a senior official acting on their behalf. If a modification, removing an operational purpose or any part of the authorised interference, is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it. If at any time the Secretary of State, or a senior official acting on their behalf, considers that a specified operational purpose is no longer necessary in the interests of the statutory purposes listed on the warrant, they shall modify the warrant to remove that operational purpose.

5.36 The modification process for bulk equipment interference requires the same level of authorisation as an application for a new bulk equipment interference warrant. When applying to modify an existing warrant, both the warrant applicant and Secretary of State should consider whether the requested modification to the warrant remains within the scope of the original warrant. If the modification is considered to be outside of the scope of the original arrant a new warrant should be sought.

5.37 A bulk equipment interference warrant authorises a two stage process; the acquisition of material, followed by the selection for examination of the material collected under the warrant. There will be limited circumstances where it may no longer be necessary, or possible, to continue the first stage of this process. In such circumstances, it may continue to be necessary and proportionate to select for examination the material collected under that warrant. The Act therefore provides that a bulk equipment interference warrant can be modified such that it no longer authorises the acquisition of material but continues to authorise selection for examination.

Urgent modification of a bulk equipment interference warrant

5.38 Section 174 of the Act makes provision for cases in which modifications of a bulk equipment interference warrant are required urgently. A modification will only be considered urgent if there is a very limited window of opportunity to act, as described in paragraph 4.504.50 of this code. The modifications that can be made urgently to a bulk equipment interference warrant are:

- to add or vary or remove an operational purpose specified on the warrant, for which material obtained under the warrant may be selected for examination; and
- to add to or vary or remove any part of the description of the conduct described in the equipment warrant.

5.39 In these cases the Secretary of State may make the urgent modification but it must be reviewed by a judicial commissioner within five working days. The Secretary of State must personally authorise the modification. Where possible, the Secretary of State will also sign the modification instrument. If this is not possible, the modification instrument may be signed by a senior official after the case, including considerations of necessity and proportionality, has been considered and approved by the Secretary of State. The Act restricts urgent modifications to bulk equipment interference warrants in this way to cases where the Secretary of State has expressly authorised the issuing of the warrant and requires the warrant to contain a statement to that effect.

5.40 In the event that the judicial commissioner does not agree to the urgent modification, the activity conducted under the urgent modification remains lawful. The judicial commissioner may authorise further interference, but only in the interest of ensuring that anything being done by virtue of the modification is stopped as soon as possible.

5.41 The urgent modification will only last for a maximum of five working days following its implementation unless renewed. If it is renewed it expires after six months, in the same way as non-urgent modifications of targeted equipment interference warrants.

Renewal of a bulk equipment interference warrant

5.42 The Secretary of State may renew a bulk equipment interference warrant at any point before its expiry date (section 172 of the Act). Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 5.9 above. In particular, the applicant must give an assessment of the value of the equipment interference to date and explain why it is considered that the interference continues to be necessary in the interests of national security as well as, where applicable, either or both of the purposes in section 165(2), and why it is considered that the conduct authorised by the warrant continues to be proportionate.

5.43 In deciding to renew a bulk equipment interference warrant, the Secretary of State must also consider that the examination of material obtained under it continues to be necessary for one or more of the specified operational purposes, and that any examination of that material for these purposes is necessary for one or more of the statutory purposes on the warrant.

5.44 In the case of a renewal of a bulk equipment interference warrant that has been modified so that it no longer authorises or requires the acquisition of material, it is not necessary for the Secretary of State to consider that the acquisition of such material continues to be necessary before making a decision to renew the warrant.

5.45 Where the Secretary of State is satisfied that the warrant continues to meet the requirements of the Act, the Secretary of State may renew it. The renewed warrant is valid for six months from the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed. For example, where a warrant is due to expire on 1 January, and the Secretary of State and Judicial Commissioner are satisfied that it should be renewed, the renewed warrant will be expire on 2 July.

5.46 In those circumstances where the assistance of a CSP or other person has been sought, a copy of the warrant renewal instrument will be forwarded to all those on whom a copy of the original warrant instrument has been served, providing they are still actively assisting. A renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

Warrant cancellation

5.47 The Secretary of State, or a senior official acting on their behalf, may cancel a bulk equipment interference warrant at any time. Such persons must cancel a warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary in the interests of national security or the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct. Such persons must also cancel a warrant if, at any time before its expiry date, he or she is satisfied that the examination of material acquired under the warrant is no longer necessary for any of the operational purposes specified on the warrant.

5.48 Equipment interference agencies will therefore need to keep their warrants under regular review and must notify the Secretary of State if they assess that the equipment interference is no longer necessary. In practice, the responsibility to cancel a warrant will be exercised by a senior official in the warrant issuing department on behalf of the Secretary of State.

5.49 The Act requires the person to whom a warrant is addresses to secure that anything in the process of being done under the warrant stops as soon as possible, so far as is reasonably practicable. In some circumstances it may be impossible, or not reasonably practicable, to cease all elements of interference upon cancellation of a warrant. In deciding what ought to be done to achieve this, an equipment interference agency must consider what further interference with equipment and privacy might be necessary and whether it is proportionate to undertake it (without further authorisation) in order to stop the original activity. In cases of doubt equipment interference agencies may seek advice from the IPC.

5.50 The cancellation instrument will be addressed to the equipment interference agency to whom the warrant was issued. A copy of the cancellation instrument should be sent to those providers or other persons, if any, who have given effect to the warrant during the preceding twelve months.

Examination Safeguards

Safeguards when selecting for examination content obtained under a bulk equipment interference warrant

5.51 Section 179 of the Act provides specific safeguards relating to the selection for examination of material acquired under a bulk equipment interference warrant. References to examination of material are references to it being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.

5.52 Sections 179(1) and (2) make clear that selection for examination may only take place for one or more of the operational purposes that are specified on the warrant. Operational purposes limit the purposes for which data collected under the warrant can be selected for examination, rather than limiting the information which can be examined per se, and no official is permitted to gain access to the data other than as permitted by these purposes. Material selected for examination for an operational purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained on any relevant ground.

5.53 Section 179 makes clear that operational purposes must relate to one or more of the statutory purposes specified on the warrant. However, it is not sufficient under the Act for operational purposes simply to use the wording of one of the statutory purposes. They must include more detail to ensure that material can only be selected for examination for specific reasons. Operational purposes provide the Secretary of State and the Judicial Commissioner with a more granular understanding of the purposes for which the material will be selected for examination.

5.54 Although bulk equipment interference warrants are authorised for the purpose of acquiring overseas-related communications, equipment data or other information, section 179(5) of the Act makes clear that a bulk equipment interference warrant can authorise the acquisition of material that is not overseas-related to the extent this is necessary in order to acquire the overseas-related material to which the warrant relates. Operational purposes specified on bulk equipment interference warrants may therefore include purposes that enable the selection for examination of material of individuals in the UK. The safeguards in section 179 of the Act ensure that where protected material is selected for examination by any criteria referable to an individual known to be in the British Islands at that time, a targeted examination warrant must be obtained under Part 5 of the Act authorising the selection for examination of that material.

5.55 The security and intelligence agencies need to retain the operational agility to respond to developing and changing threats and the range of operational purposes that may need to be specified on a bulk warrant needs to reflect this. New operational purposes will therefore be required over time. The Act provides for a bulk equipment interference warrant to be modified such that the operational purposes specified on it can be added to or varied by the Secretary of State with approval from a Judicial Commissioner. In addition, a senior official may modify a bulk equipment interference warrant to remove one or more operational purposes.

5.56 In line with this, the security and intelligence agencies will need to ensure the full range of their bulk warrants are relevant to the current threat picture and, where applicable, the intelligence priorities set by the National Security Council. They will need to identify operational purposes that need to be added to or removed from bulk warrants, including in urgent circumstances. This would be done through the modifications process set out at Section 173 of the Act.

5.57 Some operational purposes that may need to be specified on a bulk warrant will be consistent across the three agencies, although some purposes will be relevant to a particular agency or two of the three, reflecting differences in their statutory functions. Operational purposes should as far as possible be consistent across the bulk capabilities provided for by the Act.

5.58 As well as being necessary for one of the operational purposes, any selection for examination of material must be necessary and proportionate.

5.59 In general, automated systems must, where technically possible, be used to effect the selection in accordance with section 179 of the Act. As an exception, material acquired through bulk equipment interference may be accessed by a limited number of specifically authorised staff without having been processed or filtered by the automated systems. Such access may only be permitted to the extent necessary to determine whether the content falls within the main categories to be selected under the specified operational purposes, or to ensure that the methodology being used remains up to date and effective. Such checking must itself be necessary on the grounds specified in sections 165(1)(b) and 165(2) of the Act. Once those functions have been fulfilled, any copies made of the content for those purposes must be destroyed in accordance with section 177(5) of the Act. Such checking by officials should be kept to an absolute minimum; whenever possible, automated selection techniques should be used instead. Checking will be kept under review by the IPC during his or her inspections.

5.60 Communications and information collected under a bulk equipment interference warrant should be selected for examination only by authorised persons who receive mandatory training regarding the provisions of the Act and specifically the operation of section 179 and the requirements of necessity and proportionality. These requirements and procedures must be set out in internal guidance provided to all authorised persons and the attention of all authorised persons must be specifically directed to the statutory safeguards. All authorised persons must be appropriately vetted.

5.61 Prior to an authorised person being able to select for examination, a record should be created setting out why access to the content is necessary in pursuance of section 179 and the applicable operational purpose(s), and why such access is proportionate. Save where the content or automated systems are being checked as described in paragraph 5.59, the record must indicate, by reference to specific factors, the content to which access is being sought and systems should, to the extent possible, prevent access to the content unless such a record has been created. Where it is anticipated that the selection for examination is likely to give rise to collateral intrusion into privacy, the reasons this is considered proportionate, and any steps to minimise it, must also be recorded. All records must be retained in accordance with agreed policy for the purposes of subsequent examination or audit.

5.62 Access to the content as described in paragraph 5.61 must be limited to a defined period of time, although access may be renewed. If access is renewed, the record must be updated with the reason for the renewal. Systems must be in place to ensure that if a request for renewal is not made within that period, then no further access will be granted.

5.63 Periodic audits should be carried out to ensure that the requirements set out in section 179 of the Act are being met. These audits must include checks to ensure that the records requesting selection for examination have been correctly compiled, and specifically, that the content requested falls within operational purposes the Secretary of State has considered necessary for examination. Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management and any breaches of safeguards must be reported to the IPC. All intelligence reports generated by the authorised persons must be subject to a quality control audit.

5.64 The Secretary of State must ensure that the safeguards are in force before any interference under a bulk equipment interference warrant can begin. The IPC is under a duty to review the adequacy of the safeguards.

5.65 More than one operational purpose may be specified on a single bulk warrant; this may, where the necessity and proportionality test is satisfied, include all the operational purposes currently specified on the central list maintained by the heads of the security and intelligence agencies.

5.66 Other than in exceptional circumstances, it will always be necessary for every warrant application to require the full range of operational purposes to be specified in relation to the selection for examination of equipment data obtained under bulk equipment interference warrants.

Selection for examination of protected material in breach of the section 179(4) prohibition

5.67 Any selection for examination of protected material must also meet the selection conditions set out at section 179(3) and (4). Section 179(4) prohibits the selection of protected material for examination using criteria referable to an individual known to be in the British Islands in order to identify the content of communications content or private information of that individual. Selection in breach of this prohibition is only permitted where:

- A targeted examination warrant has been issued under Part 5 authorising the examination of the protected material, or
- The selection for examination in breach of the prohibition is authorised by section 170(5).

5.68 Selection in breach of the prohibition in section 179(4) of the Act may be authorised by section 179(5) authorisation. Subsection (5) addresses cases where there is a change of circumstances such that a person whose material is being selected for examination enters or is discovered to be in the British Islands, for example where a member of an international terrorist or organised crime group travels into the UK. To enable the selection for examination to continue, sections 179(5) and 179(6) of the Act provide for a senior official to give a written authorisation for the continued selection for examination of protected material relating to that person for a period of five working days. Any selection for examination after that point will require the issue of a targeted examination warrant, issued by the Secretary of State and approved by a Judicial Commissioner. Where selection for examination is undertaken in accordance with section 179(5), the Secretary of State must be notified.

6 Implementation of warrants and Communication Service Provider compliance

6.1 After the decision to issue a warrant has been approved by the Judicial Commissioner it will be forwarded to the person to whom it is addressed – in practice the equipment interference agency which submitted the application. The equipment interference agency will carry out the equipment interference itself, and may (in addition to acting on its own) require other persons to provide assistance in giving effect to the warrant.

6.2 Section 121 of the Act permits a number of equipment interference agencies to serve a warrant on telecommunication operators. The agencies named by the Act are:

- The Security and Intelligence Agencies;
- Defence intelligence;
- The NCA;
- The Metropolitan Police Service;
- The Police Service of Scotland;
- The Police Service of Northern Ireland; and
- Her Majesty's Revenue and Customs.

6.3 Where a copy of an equipment interference warrant has been served on anyone providing a telecommunications service, or who has control of a telecommunication system in the UK, that person is under a duty to take all such steps for giving effect to the warrant as are notified to him or her by or on behalf of the person to whom the warrant is addressed. For the purpose of requiring any person to provide such assistance, the equipment interference agency may serve a copy of the warrant on any person, inside or outside the UK, who is required to provide assistance in relation to that warrant[21].

6.4 Section 120 of the Act[22] provides that service of a copy of a warrant on a person outside the UK may (in addition to electronic or other means of service) be effected in any of the following ways:

- By serving it at the person's principal office within the UK or, if the person does not have an office in the UK, at any place in the UK where the person carries on business or conducts activities;
- At an address in the UK specified by the person for service;
- By making it available for inspection at a place in the UK (if neither of the above two methods are reasonably practicable). The person to whom the warrant is addressed must take steps to bring the contents of the warrant to the attention of the relevant person.

[21] See section 121 of the Act.

[22] By virtue of section 176 of the Act, section 120 (service of warrants) applies in relation to bulk equipment interference warrants as it applies in relation to targeted warrants.

Provision of reasonable assistance to give effect to a warrant

6.5 Any CSP, or any person who offers or provides a telecommunications service to the UK or has control of a telecommunications system located wholly or partly in the UK, may be required to provide assistance in giving effect to an equipment interference warrant. A warrant can only be served on a person who is considered by the implementing authority to be able to provide the assistance required by the warrant. . For the avoidance of doubt, in appropriate circumstances, this does not prevent equipment interference agencies and providers working co-operatively together (without the need for service of a copy of an equipment interference warrant in accordance with section 121).

6.6 In the case of the Security and Intelligence Agencies and Defence Intelligence, the Act places a requirement on providers served with a warrant, issued by the Secretary of State or the Scottish Ministers, to take all reasonably practicable steps for giving effect to the warrant as are notified to them (section 121(5)).

6.7 In the case of warrants issued to specified law enforcement officers, the Act places a requirement on providers to take all such steps for giving effect to the warrant as were approved by the Secretary of State and as are notified to the provider by or on behalf of the law enforcement officer to whom the warrant is addressed (section 121(2)). Section 121(2) and (4) ensures that the steps that providers are required to take are limited to those that the Secretary of State has expressly approved as necessary and proportionate to what is sought to be achieved by them. Equipment interference agencies should endeavour to work co-operatively with persons providing assistance in giving effect to warrants, and should seek to implement warrants on a collaborative basis. Assistance sought will typically comprise (but may not be limited to) the provision of infrastructure by a relevant CSP, or details about the technical specification of relevant equipment.

6.8 When requesting assistance that would involve employees of a telecommunication service provider, the equipment interference agency and the Secretary of State should consider during the authorisation process:

- What measures should be taken by the equipment interference agency to best instruct and support any CSP employees required to assist with implementation; and
- What measures should be taken to minimise any impact upon the CSP and their employees so far as is practicable.

6.9 In some cases equipment interference agencies may consider that the same material can be acquired either with assistance of a CSP or independently. The agency and issuing authority should consider the merits of either approach in the context of the specific operation, this should include the consideration of the criteria in paragraph 3.27.

6.10 The steps which may be required by CSPs are limited to those which it is reasonably practicable to take (section 121(5)). What is reasonably practicable will be considered on a case-by-case basis, taking into account the individual circumstances of the relevant CSP, and should be agreed after consultation between the CSP and the Government. Such consultation is likely to include consideration of a number of factors including, but not limited to, the technical feasibility and likely cost of complying with any steps notified to the CSP. As part of the consultation, the CSP may raise any other factor that they consider relevant to whether the taking of such steps is reasonably practicable. If no agreement can be reached it will be for the Secretary of State to decide whether to proceed with civil proceedings.

6.11 Where the equipment interference agency requires the assistance of a CSP in order to implement a warrant, it must provide one or more of the following to the CSP:

- A copy of the signed and dated warrant with the omission of any schedule contained in the warrant; or
- A copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant.

6.12 An optional covering document from the equipment interference agency (or the person acting on behalf of the agency) may also be provided requiring the assistance of the provider and specifying any other details as may be necessary. Contact details with respect to the equipment interference agency will either be provided in this covering document or will be available in the handbook provided to all CSPs who maintain a technical capability.

6.13 Section 94(5)(b) of the Act makes lawful any conduct undertaken by a person in pursuance of requirements imposed by or on behalf of a person to whom an equipment interference warrant is addressed. This therefore authorises activity taken by CSPs in giving effect to a warrant that would otherwise constitute an offence under the CMA, Data Protection legislation or other relevant legislation. Where assistance is required that - but for section 94(5)(b) - would constitute an offence, the issuing authority and, if not the issuing authority, the Secretary of State should consider ways in which the warrant can be executed so as to minimise such activity and the need to rely on section 94(5)(b); this is part of the consideration of whether the activity authorised by the warrant is proportionate and cannot be achieved by less intrusive means

Contribution of costs for giving effect to an equipment interference warrant

6.14 Section 225 of the Act recognises that CSPs incur expenses in complying with requirements in the Act, including equipment interference in response to requests under Part 5 of the Act. The Act, therefore, allows for appropriate payments to be made to them to cover these costs.

6.15 Public funding and support is made available to CSPs to ensure that they can provide, outside of their normal business practices, an effective and efficient response to public authorities' necessary, proportionate and lawful requirements in support of their investigations and operations in the interests of national security, to protect the public and to bring to justice those who commit crime.

6.16 It is legitimate for a CSP to seek contributions towards its costs which may include an element providing funding of those general business overheads required in order to facilitate the timely implementation of an equipment interference warrant. This is especially relevant for CSPs which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke systems. However, this category of costs will not in most cases include specific staff benefits or arrangements made in line with the terms and conditions of employment, such as pension payments. Such matters are arranged between the employer and employee and the Government does not accept liability for such costs.

6.17 Contributions may also be appropriate towards costs incurred by a CSP which needs to update its systems to maintain, or make more efficient, its processes. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements.

6.18 Any CSP seeking to recover appropriate contributions towards its costs should make available to the Government such information as the Government requires in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the CSP.

6.19 Any CSP that has claimed contributions towards costs may be required to undergo a Government audit before contributions are made. This is to ensure that expenditure has been incurred for the stated purpose. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

7 Maintenance of a technical capability

7.1 CSPs may be required under section 229 of the Act to provide a technical capability to give effect to interception, equipment interference, bulk acquisition warrants or communications data acquisition authorisations. The purpose of maintaining a technical capability is to ensure that, when a warrant is served, companies can give effect to it securely and quickly. Small companies (with under 10,000 users) will not be obligated to provide a permanent technical capability, although they may be obligated to give effect to a warrant.

7.2 The Secretary of State may give a relevant CSP a "technical capability notice" imposing on the relevant operator obligations specified in the notice, and requiring the person to take all steps specified in the notice. In practice, notices will only be given to CSPs that are likely to be required to give effect to warrants or authorisations on a recurrent basis.

7.3 The obligations that the Secretary of State considers reasonable to impose on CSPs are set out in regulations made by the Secretary of State and approved by Parliament, and may include (amongst others) obligations set out at section 229(4) of the Act:

- Obligations to provide facilities or services of a specified description;
- Obligations relating to apparatus owned or operated by a relevant operator;
- Obligations relating to the removal of electronic protection applied by or on behalf of the relevant operator on whom the obligation has been placed to any communications or data;
- Obligations relating to the security of any telecommunications services provided by the relevant operator; and
- Obligations relating to the handling or disclosure of any information.

7.4 An obligation placed on a CSP to remove encryption only relates to electronic protections that the company has itself applied to material (and secondary data), or where those protections have been placed on behalf of that CSP. The purpose of this obligation is to ensure that the requested material can be provided to the equipment interference agencies in readable form. References to protections applied on behalf of the CSP include circumstances where the CSP has contracted a third party to apply electronic protections to a telecommunications service provided by that CSP to their customers.

7.5 In the event that a number of CSPs are involved in the provision of a service, the obligation to provide a capability, and to remove encryption, will be placed on the CSP which has the technical capability to give effect to the notice and on whom it is reasonable practicable to impose these requirements. It is possible that more than one CSP will be involved in the provision of the capability, particularly if more than one CSP applies electronic protections to the relevant material.

7.6 While an obligation to remove encryption may only relate to protections applied by or on behalf of the company on whom the obligation is placed, there will also be circumstances where a CSP removes encryption from communications for their own business reasons. Where this is the case an equipment interference agency will also require the CSP, where applicable and when served with a warrant, to provide those communications in an intelligible form.

Consultation with service providers

7.7 Before giving a notice, the Secretary of State must consult the CSP[23]. In practice, informal consultation is likely to take place long before a notice is given. The Government will engage with CSPs who are likely to be subject to a notice in order to provide advice and guidance, and prepare them for the possibility of receiving a notice.

7.8 In the event that the giving of a notice to a CSP is deemed necessary and proportionate, the Government will take steps to consult the CSP formally before the notice is given. Should the CSP have concerns about the reasonableness, cost or technical feasibility of requirements to be set out in the notice, these should be raised during the consultation process. Any concerns outstanding at the conclusion of these discussions will be presented to the Secretary of State and will form part of the decision making process.

Matters to be considered by the Secretary of State

7.9 Following the conclusion of consultation with a CSP, the Secretary of State will decide whether to give a notice. This consideration should include all the aspects of the proposed notice. It is an essential means of ensuring that the notice is necessary and proportionate to what is sought to be achieved and that proper processes have been followed.

7.10 As part of the decision the Secretary of State must take into account, amongst other factors, the matters specified in section 231(3):

- The likely benefits of the notice – this may take into account projected as well as existing benefits.
- The likely number of users (if known) of any service to which the notice relates – this will help the Secretary of State to consider both the level of intrusion on customers but also the likely benefits of the technical capability notice.
- The technical feasibility of complying with the notice – taking into account any representations made by the CSP and giving specific consideration to any obligations in the notice to remove electronic protections (as described at 231(4)).
- The likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the CSP as part of the notice, such as those relating to security. This should also include specific consideration to the likely cost of complying with any obligations in the notice to remove electronic protections. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money.
- Any other effect of the notice on the CSP – again taking into account any representations made by the company.

7.11 In addition to the points above, the Secretary of State should consider any other issue which is considered to be relevant to the decision. Section 2 of the Act also requires the Secretary of State to give regard to the following when giving, varying or revoking a notice:

- whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means,
- the public interest in the integrity and security of telecommunication systems and postal services, and
- any other aspects of the public interest in the protection of privacy.

[23] See section 218(2).

7.12 The Secretary of State may give a notice after considering of the points above if he or she considers that the notice is necessary, and that the conduct required is proportionate to what is sought to be achieved. The obligations set out in the notice must be reasonable, and the Secretary of State must be satisfied that the communications service providers are capable of providing the necessary technical assistance.

7.13 Before the notice may be given, a Judicial Commissioner must approve the Secretary of State's decision to give a notice. In deciding whether to approve the Secretary of State's decision to give a relevant notice, a Judicial Commissioner must review the Secretary of State's conclusions regarding the necessity of the notice and the proportionality of the conduct required by the notice in relation to what is sought to be achieved.

Giving a notice

7.14 Once a notice has been signed by the Secretary of State and approved by the Judicial Commissioner, arrangements will be made for this to be given to the CSP. During the consultation process, it will be agreed who within the company should receive the notice and how it should be issued (i.e. electronically or in hard copy). If no recipient is agreed, then the notice will be issued to a senior executive within the company.

7.15 Section 229(8) provides that obligations may be imposed on, and technical capability notices given to, persons located outside the UK and may require things to be done or not done outside the UK. Where a notice is to be given to a person outside the UK, the notice may (in addition to electronic or other means of service) be given to the CSP[24]:

- By delivering it to the person's principal office within the UK or, if the person does not have an office in the UK, to any place in the UK where the person carries on business or conducts activities; or
- At an address in the UK specified by the person.

7.16 The person or company to whom a notice is given will be provided with a handbook which will contain the basic information they will require to respond to requests for reasonable assistance in relation to the acquisition of material.

7.17 As set out in section 229(7)), the notice will specify the period within which the CSP must undertake the steps specified in the notice. It will often be the case that a notice will require the creation of dedicated systems. The time taken to design and construct such a system will be taken into account and, accordingly, different elements of the notice may take effect at different times.

7.18 A person to whom a technical capability notice is given is under a duty to comply with the notice. In respect of a technical capability notice to give effect to equipment interference warrants, the duty to comply with a technical capability notice is enforceable against a person in the UK by civil proceedings by the Secretary of State[25]. The duty to comply with a technical capability notice to give effect to equipment interference warrants is enforceable against a person in the UK and a person outside the UK by civil proceedings by the Secretary of State[26].

[24] See section 231(6).

[25] See section 231(10)(a).

[26] See section 231(10)(b).

Disclosure of technical capability notices

7.19 The Government does not publish or release identities of those subject to a technical capability notice, as to do so may identify operational capabilities or harm the commercial interests of companies acting under a notice. Should criminals become aware of the capabilities of law enforcement, they may alter their behaviours and change CSP, making it more difficult to detect their activities of concern.

7.20 Any person to whom a technical capability notice is given, or any person employed or engaged for the purposes of that person's business, is under a duty not to disclose the existence and contents of that notice to any person[27].

7.21 Section 231(8) of the Act provides for the person to disclose the existence and content of a technical capability notice with the permission of the Secretary of State. Such circumstances are likely to include disclosure:

- To a person (such as a system provider) who is working with the CSP to give effect to the notice;
- To relevant oversight bodies;
- To regulators, in exceptional circumstances where information relating to a capability may be relevant to their enquiries;
- To other CSPs subject to a technical capability notice to facilitate consistent implementation of the obligations; and
- In other circumstances notified to and approved in advance by the Secretary of State.

7.22 Section 125 of the Act sets out the meaning of “excepted disclosure” and the circumstances in which disclosure made in relation to a warrant is permitted. This includes when a disclosure is made, not in relation to a particular warrant but in relation to equipment interference warrants in general. This includes provision for CSPs to be able to publish information in relation to the number of warrants they have given effect to. In order to ensure that this does not reveal sensitive information that could undermine the ability of the security and intelligence and law enforcement agencies to do their job, further information on the way in which this information can be published is set out in regulations. The regulations make clear that statistical information can be published on the number of warrants that a CSP has given effect to within a specified range rather than the exact number.

Regular review

7.23 The Secretary of State must keep technical capability notices under review. This helps to ensure that the notice itself, or any of the requirements specified in the notice, remain necessary and proportionate.

7.24 It is recognised that, after a notice is given, the CSP will require time to take the steps outlined in the notice and develop the necessary capabilities. Until these capabilities are fully operational, it will be difficult to assess the benefits of a notice. As such, the first review should not take place until after these are in place.

7.25 A review of a technical capability notice will take place at least once every two years once capabilities are in place. However, the exact timing of the review is at the Secretary of State’s discretion.

[27] See section 218(8).

7.26 A review may be initiated earlier than scheduled for a number of reasons. These include:

- a significant change in demands by the equipment interference agencies that calls into question the necessity and proportionality of the notice as a whole, or any element of the notice;
- a significant change in the CSP's activities or services; or
- a significant refresh or update of CSP's systems.

7.27 The process for reviewing a notice requires the Secretary of State to consult the CSP to determine whether the notice remains necessary and proportionate.

7.28 A review may recommend the continuation, variation or revocation of a notice. The relevant CSP and the equipment interference agencies will be notified of the outcome of the review.

Variation of technical capability notices

7.29 The communications market is constantly evolving and CSPs subject to technical capability notices will often launch new services.

7.30 CSPs subject to a technical capability notice must notify the Government of new products and services in advance of their launch, in order to allow consideration of whether it is necessary and proportionate to require the CSP to provide a technical capability on the new service.

7.31 Small changes, such as upgrades of systems which are already covered by the existing notice, can be agreed between the Government and CSP in question. However, significant changes will require a variation of the technical capability notice.

7.32 Section 232 of the Act provides that technical capability notices can be varied by the Secretary of State. There are a number of reasons why a notice might be varied. These include:

- a CSP launching new services;
- changing law enforcement demands and priorities;
- a recommendation following a review (see paragraph 7.28 above); or
- to amend or enhance the security requirements.

7.33 Where a CSP has changed name, for example as part of a rebranding exercise or due to a change of ownership, the Secretary of State, in consultation with the CSP, will need to consider whether the existing notice should be varied.

7.34 Before varying a notice, the Secretary of State will consult the equipment interference agencies to understand the operational impact of any change to the notice, and the CSPs to understand the impact on them, including any technical implications. Once this consultation process is complete, the Secretary of State will consider whether it is necessary to vary the notice and whether the new requirements imposed by the notice as varied are proportionate to what is sought to be achieved by that conduct.

7.35 Further detail on the consultation process and matters to be considered by the Secretary of State can be found above at paragraph 7.7.

7.36 Once a variation has been agreed by the Secretary of State, arrangements will be made for the CSP to receive notification of this variation and details of the timeframe in which the variation needs to be enacted by the CSP. The time taken to implement these changes will be taken into account and, accordingly, different elements of the variation may take effect at different times.

Revocation of technical capability notices

7.37 A technical capability notice must be revoked (in whole or in part) if it is no longer necessary or proportionate to require a CSP to provide a technical capability.

7.38 Circumstances where it may be appropriate to revoke a notice include where a CSP no longer operates or provides the services to which the notice relates, where operational requirements have changed, or where such requirements would no longer be necessary or proportionate.

7.39 The revocation of a technical capability notice does not prevent the Secretary of State issuing a new technical capability notice, covering the same, or different, services to the same CSP in the future should it be considered necessary and proportionate to do so.

Referral of technical capability notices

7.40 The Act includes clear provisions for CSPs to request a review of the requirements placed on them in a technical capability notice should they consider these to be unreasonable. A person may refer the whole or any part of a technical capability notice back to the Secretary of State for review under section 233 of the Act.

7.41 The circumstances and timeframe within which a CSP may request a review are set out in regulations made by the Secretary of State and approved by Parliament. These circumstances include opportunities for a CSP to refer a notice for review following the receipt of a new notice or the notification of a variation to a notice. Details of how to submit a notice to the Secretary of State for review will be provided either before or at the time the notice is served.

7.42 Before deciding the review, the Secretary of State must consult and take account of the views of the Technical Advisory Board (TAB) and a Judicial Commissioner. The Board must consider the technical requirements and the financial consequences of the notice for the person who has made the referral. The Commissioner will consider whether the notice is proportionate.

7.43 The Commissioner and the TAB must give the relevant CSP and the Secretary of State the opportunity to provide evidence and make representations to them before reaching their conclusions. Both bodies must report these conclusions to the person who made the referral and the Secretary of State.

7.44 After considering reports from the TAB and the Commissioner, the Secretary of State may decide to vary, withdraw or confirm the effect of the notice. Where the Secretary of State decides to confirm or vary the notice, the Investigatory Powers Commissioner must approve the decision. Until the Secretary of State's decision is approved, there is no requirement for the CSP to comply with the notice so far as referred. The CSP will remain under obligation to provide assistance in giving effect to an equipment interference warrant, as set out in section 121 of the Act.

Contribution of costs for the maintenance of a technical capability

7.45 Section 225 of the Act recognises that CSPs incur expenses in complying with requirements in the Act, including notices to maintain permanent capabilities under Part 9. The Act, therefore, allows for appropriate payments to be made to them to cover these costs.

7.46 CSPs that are subject to a technical capability notice under Part 9 of the Act are able to recover a contribution towards these costs to ensure that they can establish, operate and maintain effective, efficient and secure infrastructure and processes in order to meet their obligations under a technical capability notice and the Act.

7.47 Any contribution towards these costs must be agreed by the Government before work is commenced by a CSP and will be subject to the Government considering, and agreeing, the technical capability proposed by the CSP.

7.48 Costs that may be recovered could include those related to the procurement or design of systems required to acquire material, their testing, implementation, continued operation and, where appropriate, sanitisation and decommissioning. Certain overheads may be covered if they relate directly to costs incurred by CSPs in complying with their obligations outlined above. This is particularly relevant for CSPs that employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems. However, this category of costs will not in most cases include specific staff benefits or arrangements made in line with the terms and conditions of employment, such as pension payments. Such matters are arranged between the employer and employee and the Government does not accept liability for such costs.

7.49 Contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the use of such services. However, where a CSP expands or changes its network for commercial reasons, it is expected to meet any capital costs that arise.

General considerations on appropriate contributions

7.50 Any CSP seeking to recover appropriate contributions towards its costs should make available to the Government such information as the Government requires in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the CSP.

7.51 As costs are reimbursed from public funds, CSPs should take into account value for money when procuring, operating and maintaining the infrastructure required to comply with a notice. As changes to business systems may necessitate changes to systems, CSPs should take this into account when altering business systems and must notify the Government of proposed changes.

7.52 Any CSP that has claimed contributions towards costs may be required to undergo a Government audit before contributions are made. This is to ensure that expenditure has been incurred for the stated purpose. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

Power to develop compliance systems

7.53 In certain circumstances it may be more economical for products to be developed centrally, rather than CSPs or public authorities creating multiple different systems to achieve the same end. Where multiple different systems exist, it can lead to increased complexity, delays and higher costs when updating systems (for example, security updates).

7.54 Section 226 of the Act provides a power for the Secretary of State to develop compliance systems. This power could be used, for example, to develop consistent systems for use by CSPs to acquire material. Such systems could operate in respect of multiple powers under the Act.

7.55 Where such systems are developed for use by CSPs, the Government will work closely with CSPs to ensure the systems can be properly integrated into their networks. CSPs using such systems will have full sight of any access or processing of their data carried out by such systems.

Principles of data security, integrity and disposal of systems

Legal and regulatory compliance

7.56 All equipment interference systems and practices must be compliant with relevant legislation.

7.57 All systems and practices must comply with any security policies and standards in place in relation to equipment interference. This may include any policies and standards issued by the Home Office. These further requirements are unlikely to be publicly available as they may contain specific details of security infrastructure or practices, disclosure of which could create additional security risks.

Information security policy & risk management

7.58 Each communications service provider must develop a security policy. This policy document should describe the internal security organisation, the governance and authorisation processes, access controls, necessary training, the allocation of security responsibilities, and policies relating to the security and integrity of capabilities. Each communications service provider must also develop security operating procedures. A communications service provider can determine whether this forms part of, or is additional to, wider company policies.

7.59 The security policy document and security operating procedures should be reviewed regularly to ensure they remain appropriate

7.60 Each communications service provider must identify, assess and treat all information security risks, including those which relate to arrangements with external parties.

Human Resources Security

7.61 Communications service providers must clearly identify roles and responsibilities of staff, ensuring that roles are appropriately segregated to ensure staff only have access to the information necessary to complete their role. Access rights and permissions assigned to users must be revoked on termination of their employment. Such rights and permissions must be reviewed and, if appropriate, amended or revoked when staff move roles within the organisation.

7.62 Staff with access to sensitive systems and sensitive information related to warranted interference should be subject to an appropriate level of security screening. The Government sponsors and manages security clearance for certain staff working within a communications service provider to ensure the company's compliance with obligations under this legislation. Communications service providers must ensure that these staff have undergone relevant security training and have access to security awareness information.

7.63 All persons who may have access to the product of equipment interference, or need to see any reporting in relation to it, must be appropriately vetted. On an annual basis, managers must identify any concerns that may lead to the vetting of individual members of staff being reconsidered. The vetting of each individual member of staff must also be periodically reviewed.

7.64 Where it is necessary for an officer of an equipment interference agency to disclose information related to warranted equipment interference to a communications service provider operating under a technical capability notice, it is the former's responsibility to ensure that the recipient has the necessary security clearance.

Maintenance of Physical Security

7.65 There should be appropriate security controls in place to prevent unauthorised access to sensitive information. Access to the locations where the systems are both operated and hosted must be controlled such that access is limited to those with the relevant security clearance and permissions.

7.66 Equipment used to for the purpose of warranted equipment interference must be sanitised and securely disposed of at the end of its life[28].

Operations management

7.67 Systems used for equipment interference should be subject to a documented change management process, including changes to third party suppliers, to ensure that no changes are made to systems without assessing the impact on the security of the product.

7.68 Communications service providers must also put in place a patching policy to ensure that regular patches and updates are applied to any equipment interference capabilities or support systems as appropriate. Such patches and updates will include anti-virus, operating systems, application and firmware. The patching policy including timescale in which patches must be applied, must be agreed with the Home Office.

7.69 Communications service providers should ensure that, where encryption is in place in equipment interference systems, any encryption keys are subject to appropriate controls, in accordance with the appropriate security policy.

7.70 Network infrastructure, services, media, and system documentation must be stored and managed in accordance with the security policy and an inventory of all assets should be maintained together with a clear identification of their value and ownership. All assets must be clearly labelled.

Access Controls

7.71 Where a communication service provide has access to any equipment that forms part of a technical capability, they must ensure that registration and access rights, passwords and privileges for access to dedicated equipment interference systems and associated documentation are managed in accordance with their security policy. They must also ensure that users understand and formally acknowledge their security responsibilities.

7.72 Access to operating systems must be locked down to an appropriate standard and any mobile computing (i.e. offsite access to communications service provider systems from non-secure locations) must be subject to appropriate policies and procedures if permitted. Accordingly any remote access for diagnostic, configuration and support purposes must be controlled.

7.73 Access should be provided to relevant oversight bodies where necessary for them to carry out their functions.

Additional requirements relating to the disposal of systems

7.74 The legal requirement to ensure deleted data is impossible to access must be taken into account when disposing of any system, or component of a system, which reaches the end of its service life.

[28] Please see 8.91 for further details on the disposal of equipment interference systems.

7.75 If the equipment is to be re-used, it must be securely sanitised by means of overwriting using a Government-approved product. If the equipment is not to be re-used immediately, it must be securely stored in such a way that it may only be re-used or disposed of appropriately.

7.76 If the equipment is to be finally disposed of, it must be securely sanitised by means of physical destruction by a Government-approved supplier.

7.77 Sanitisation or destruction of information used to identify relevant equipment must include retained copies for back-up and recovery, and anything else that stores duplicate data within the communications service provider's system, unless retention of this is otherwise authorised by law.

8 Handling of information, general safeguards and sensitive professions

Overview

8.1 This chapter provides general guidance on the processing, retention, disclosure, deletion and destruction of all material obtained by the equipment interference agencies pursuant to all equipment interference warrants. The additional safeguards which apply to the examination of such material obtained under a bulk equipment interference warrant are explained in chapter 6 of this code.

8.2 All material obtained under the authority of an equipment interference warrant must be handled in accordance with safeguards which the Secretary of State, Scottish Minister or law enforcement chief considers to be satisfactory[29]. These safeguards are made available to the IPC, and they must meet the requirements of sections 122 and 177 of the Act which are set out below. In addition, the safeguards in 179 apply to the selection for examination of material obtained under bulk equipment interference warrants. Any breach of these safeguards must be reported to the IPC. The equipment interference agencies must keep their internal safeguards under periodic review to ensure that they remain up-to-date and effective. During the course of such periodic reviews, the agencies must consider whether more of their internal arrangements might safely and usefully be put into the public domain.

8.3 In any case where communications, equipment data or other information are obtained under sections 5 or 7 of the 1994 Act or Part 3 of the 1997 Act, equipment interference agencies must handle the material so obtained in accordance with the safeguards set out in Covert Surveillance and Property Interference Code. Compliance with these safeguards will ensure that the relevant service handles the material in accordance with safeguards equivalent to those set out in chapter 8 of this code[30].

Use of material as evidence

8.4 Subject to the provisions in chapter 8 of this code, material obtained through equipment interference may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996, the Criminal Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984[31] and the Human Rights Act 1998.

[29] Before issuing a targeted or bulk equipment interference warrant, the issuing authority must be satisfied that such arrangements are in force in relation to the warrant: see sections 97(1)(c) and 1657(1)(e).

[30] The Covert Surveillance and Property Interference Code will be updated prior to implementation of the Act.

[31] And section 76 of the Police and Criminal Evidence (Northern Ireland) Order 1989.

8.5 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure test applied under the Criminal Procedure and Investigations Act 1996 and these considerations will apply to any material acquired through equipment interference that is used in evidence'. When information obtained from equipment interference is used evidentially, the equipment interference agency should be able to demonstrate how the evidence has been recovered, and be capable of showing each process through which the evidence was obtained where appropriate to do so.

8.6 Where the product of equipment interference could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review. In the cases of the law enforcement equipment interference agencies, particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996.

8.7 The heads of the Security and Intelligence Agencies and law enforcement agencies are also under a duty to ensure that arrangements are in force to secure: (i) that no information is obtained except so far as necessary for the proper discharge of their functions; and (ii) that no information is disclosed except so far as is necessary for those functions, for the purpose of any criminal proceedings, and, in the case of SIS and the Security Service, for the other purposes specified. In the case of the Security and Intelligence Agencies the arrangements must include provision with respect to the disclosure of information obtained by virtue of sections 5 and 7 of the 1994 Act, and any information so obtained must be subject to the arrangements.

General safeguards

8.8 Sections 122 and 177 of the Act require that disclosure, copying and retention of material obtained under equipment interference warrants is limited to the minimum necessary for the authorised purposes. Something is necessary for the authorised purposes if the material:

- Is, or is likely to become, necessary on any relevant grounds as set out in section 122(7) or for any of the purposes set out in sections 165(2) – as relevant, in the interests of national security, for the purpose of preventing or detecting serious crime, for the prevention of death or injury, or for the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security, of safeguarding the economic well-being of the UK[32];
- Is necessary for facilitating the carrying out of the functions under the Act of the issuing authority or the person to whom the warrant is addressed;
- Is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal;
- Is necessary for the purposes of legal proceedings; or
- Is necessary for the performance of the functions of any person by or under any enactment.

[32] Material obtained for one purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained for another.

8.9 For the avoidance of doubt, when a security and intelligence agency obtains material under a bulk equipment interference warrant and selects for examination that material in accordance with the specified operational purposes, the selected material may be retained, copied, processed and disseminated on any relevant ground.

Reviewing warrants

8.10 Regular reviews of all warrants should be undertaken during their currency to assess the need for the equipment interference activity to continue. The results of a review should be retained for at least three years. 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.

8.11 In each case, unless specified by the issuing authority or Judicial Commissioner, the frequency of reviews should be determined by the equipment interference agency who made the application. This should be as frequently as is considered necessary and proportionate.

8.12 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 equipment interference agency should consider whether it is necessary to apply for a fresh warrant.

Dissemination of material obtained under an equipment interference warrant

8.13 The number of persons to whom any of the material is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. In the same way, only so much of the material may be disclosed as is necessary for the authorised purposes. For example, if a summary of the material will suffice, no more than that should be disclosed.

8.14 The obligations apply not just to the original agency who obtained the data, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients.

8.15 Sections 123 and 178 of the Act provide that where material obtained under an equipment interference warrant, or a copy of such material, is handed over to the authorities of a country or territory outside the UK, the issuing authority must ensure that arrangements are in force to ensure that the material is only shared if the UK agency considers that arrangements corresponding to the requirements in sections 122 and 177 (relating to minimising the extent to which material is disclosed, copied, distributed and retained) will apply to the extent that the UK agency considers appropriate. In particular, the material must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency, and must be returned to the issuing agency or securely destroyed when no longer needed.

Offence of making unauthorised disclosure

8.16 According to section 126 of the Act it is a criminal offence to make unauthorised disclosure of the existence, content or details relating to an equipment interference warrant, the existence of content of any requirement to provide assistance in giving effect to a warrant, any steps taken in pursuance of a warrant and any material derived from equipment interference. This offence applies to all parties listed in section 124 (3). The offence does not apply however if:

- The disclosure is an excepted disclosure according to section 125. For example, a law enforcement officer may be authorised by the person to whom an equipment interference warrant is addressed to disclose material acquired by equipment interference in order to carry out their functions; or
- The offence does not apply to individuals who are unaware that the disclosure of the material in question would be in breach of the duty not to make unauthorised disclosures. This could be because they are not aware that the material they are disclosing is derived from equipment interference, as it may not be identifiable as the product of equipment interference.

8.17 Section 125 (2) sets out that disclosures may be authorised by the warrant, by the person to whom the warrant is addressed or by the terms of any requirement to provide assistance in giving effect to a warrant. If the issuing authority or the person to whom the warrant is addressed intends to authorise a disclosure under this section they must first consider the safeguards set out in section 122 of the Act and paragraphs 8.13 to 8.15 of this Code.

Copying

8.18 Material may only be copied to the extent necessary for the authorised purposes. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of an equipment interference warrant, and any record which includes the identities of the persons who owned, used or were in possession of the equipment interfered with under the warrant.

Storage

8.19 Material and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. This requirement to store material securely applies to all those who are responsible for handling it, including providers. The details of what such a requirement will mean in practice for providers will be set out in the discussions they have with the Government before a technical capability notice for equipment interference is given to a person (see chapter 6 of this code).

Destruction

8.20 Material, and all copies, extracts and summaries which can be identified as the product of an equipment interference warrant, must be marked for deletion and securely destroyed as soon as possible once it is no longer needed for any of the authorised purposes.

8.21 If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid for one or more of the authorised purposes.

8.22 Any collateral material that has been acquired over the course of a testing or training exercise should be destroyed as soon as reasonably possible following the conclusion of the testing or training.

Safeguards applicable to the handling of material obtained as a result of a request for assistance

8.23 Where material is obtained by a UK equipment interference agency as a result of a request to an international partner to undertake equipment interference on its behalf, the material must be subject to the same internal rules and safeguards that apply to the same categories of material when they are obtained directly by the equipment interference agency as a result of equipment interference under the Act.

Confidential information

8.24 Particular consideration should be given in cases where material is obtained or examined under an equipment interference warrant and the subject of the obtaining or examination might reasonably assume a high degree of privacy, or where confidential information is involved. This includes where the material is legally privileged; where confidential journalistic material may be involved; where equipment interference might involve material relating to communications between a medical professional or Minister of Religion and an individual concerning the latter's health or spiritual welfare; or where material concerning communications between a Member of Parliament and another person on constituency business may be involved.

8.25 Section 106 of the Act provides additional protection for members of relevant legislatures, including Members of Parliament. The Prime Minister must approve any application where it is intended to issue a targeted equipment interference warrant or a targeted examination warrant where the purpose (or one of the purposes) of the warrant is to obtain the communications or private information of a member of a relevant legislature, apart from those approved by Scottish Ministers. The PM must also be consulted before a decision is made to renew a warrant (section 106 of the Act) and prior to making a modification of a warrant in respect of a member of a relevant legislature (section 113(3) of the Act). In a case where section 106 applies in relation to making a modification, the warrant must be approved by a Judicial Commissioner. The Prime Minister must also explicitly authorise any decision made to renew such a warrant (section 110(10) of the Act).

Material involving confidential journalistic material, confidential personal information and exchanges between a Member of Parliament and another person on constituency business

8.26 Particular consideration must also be given to cases where equipment interference includes the obtaining or the examination of material that involves confidential journalistic material, confidential personal information, or communications between a Member of Parliament and another person on constituency business.

8.27 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in material being acquired for the purposes of journalism and held subject to such an undertaking.

8.28 Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his or her physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence, or is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

8.29 Spiritual counselling is defined as conversations between an individual and a Minister of Religion acting in his or her official capacity, and where the individual being counselled is seeking, or the Minister is imparting, forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

8.30 Where the intention is to acquire confidential personal information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the acquisition of confidential personal information is likely but not intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to whether special handling arrangements are required within the equipment interference agency.

8.31 Material which has been identified as confidential information should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes. It must be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised statutory purposes.

8.32 Where confidential information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from a legal adviser within the relevant equipment interference agency and before any further dissemination of the material takes place.

8.33 Any case where confidential information is retained should be notified to the IPC as soon as reasonably practicable, as agreed with the Commissioner. Any material which has been retained should be made available to the Commissioner on request.

8.34 The safeguards set out in chapter 8 also apply to any material obtained under a bulk equipment interference warrant which is selected for examination (other than as authorised by a targeted examination warrant) and which constitutes confidential information.

Items subject to legal privilege

8.35 Section 98 of the 1997 Act describes those matters that are subject to legal privilege in England and Wales. In Scotland, those matters subject to legal privilege contained in section 412 of the Proceeds of Crime Act 2002 should be adopted. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.

8.36 Legal privilege does not apply to material held with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged items will lose its protection if, for example, the professional legal adviser is intending to hold or use the items for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

8.37 For the purposes of this code, any communication between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the items do not form part of a professional consultation of the lawyer, or there is clear and compelling evidence that the 'furthering a criminal purpose' exemption applies. Where there is doubt as to whether the items are subject to legal privilege or over whether the items are not subject to legal privilege due to the "in furtherance of a criminal purpose" exception, advice should be sought from a legal adviser within the relevant equipment interference agency.

8.38 Sections 107 and 180 of the Act provides special protections for legally privileged items. Acquiring such items (or examining items subject to legal privilege acquired under a bulk equipment interference warrant) is particularly sensitive and may give rise to issues under Article 6 (right to a fair trial) of the ECHR as well as engaging Article 8. The acquisition of items subject to legal privilege (whether deliberately obtained or otherwise) is therefore subject to additional safeguards under this code as set out from paragraph 8.35. The guidance set out may in part depend on whether matters subject to legal privilege have been obtained intentionally or incidentally to other content which has been sought.

8.39 In a case where section 107 applies in relation to making a modification, the warrant must be approved by a Judicial Commissioner

Application process for targeted equipment interference and examination warrants

8.40 Where a targeted equipment interference warrant or targeted examination warrant is likely to result in a person acquiring items subject to legal privilege, the application should include, in addition to the reasons why it is considered necessary for the interference or examination to take place, an assessment of how likely it is that items which are subject to legal privilege will be obtained or examined. In addition, it should state whether the purpose (or one of the purposes) of the interference or examination is to obtain privileged items. Where the intention is not to acquire items subject to legal privilege, but it is likely that such items will nevertheless be acquired, that should be made clear in the warrant application and the relevant agency should confirm that any inadvertently obtained items that are subject to legal privilege will be treated in accordance with the safeguards set out in this chapter and that reasonable and appropriate steps will be taken to minimise access to the items subject to legal privilege.

8.41 Where the intention is to acquire legally privileged items, the issuing authority will only issue the warrant if satisfied that there are exceptional and compelling circumstances that make the authorisation necessary. Such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb or to national security, and the interference or examination is reasonably regarded as likely to yield intelligence necessary to counter the threat.

Example: An intelligence agency may need to deliberately target legally privileged communications where the legal consultation might yield intelligence that could prevent harm to a potential victim or victims. For example, if they have intelligence to suggest that an individual is about to conduct a

terrorist attack and the consultation may reveal information that could assist in averting the attack (e.g. by revealing details about the location and movements of the individual) then they might want to target the legally privileged communications.

8.42 Further, in considering any such application, the issuing authority must believe that the proposed conduct is proportionate to what is sought to be achieved. In particular the issuing authority must consider whether the purpose of the proposed interference or examination could be served by obtaining non-privileged items. In such circumstances, the issuing authority will be able to impose additional conditions such as regular reporting arrangements, so as to be able to exercise his or her discretion on whether a warrant should continue to have effect.

8.43 Where there is a renewal application in respect of a warrant which has resulted in the obtaining of legally privileged items, that fact should be highlighted in the renewal application.

Selection for examination of legally privileged protected material under a bulk equipment warrant: requirement for prior approval by independent senior official

8.44 Where protected material obtained under a bulk equipment interference warrant is to be selected for examination according to a factor that is intended, or is likely to, result in a person acquiring items subject to legal privilege, and the selection would not breach the prohibition in section 179(4) (so a targeted examination warrant is not required), the enhanced procedure described at paragraph 8.40 and 8.43 applies.

8.45 An authorised person[33] in a public authority must notify a senior official[34] before using a factor to select any protected material for examination, where this will, or is likely to, result in the acquisition of legally privileged items. The notification must address the same considerations as described in paragraph 8.40. The senior official, who must not be a member of the public authority to whom the bulk equipment interference warrant is addressed, must in any case where the intention is to acquire items subject to legal privilege, apply the same tests and considerations as described in paragraph 8.41 and 8.42. The authorised person is prohibited from accessing the items until he or she has received approval from the senior official authorising the selection of the items subject to legal privilege.

8.46 In the event that privileged items are inadvertently and unexpectedly selected for examination (and where the enhanced procedure in paragraph 8.40 has consequently not been followed), any item so obtained must be handled strictly in accordance with the provisions of this chapter. No further privileged items may be selected for examination by reference to that factor unless approved by the senior official as set out in paragraph 8.45.

[33] See chapter 6.

[34] Senior official is defined in section 173 of the Act as “senior official” means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty’s Diplomatic Service.

Lawyers' material

8.47 Where a lawyer, acting in this capacity, is the subject of a targeted equipment interference warrant or a targeted examination warrant or whose material has otherwise been selected for examination in accordance with section 179, it is possible that a substantial proportion of the material which will be obtained or examined will be between the lawyer and his or her client(s) and will be subject to legal privilege. Therefore, in any case where the subject of a targeted equipment interference warrant, a targeted examination warrant or whose material has been selected for examination is known to be a lawyer acting in this capacity the application or notification must be made on the basis that it is likely to acquire material subject to legal privilege and the provisions in paragraphs 8.40 - 8.46 will apply, as relevant. This paragraph does not prevent an application being made on the grounds that the lawyer is under investigation for serious criminal offences.

8.48 Any such case should also be notified to the IPC during his or her next inspection and any material which has been retained should be made available to the Commissioner on request.

Handling, retention and deletion

8.49 In addition to safeguards governing the handling and retention of material as provided for in sections 122 and 177 of the Act, officials who analyse material obtained by equipment interference should be alert to any communications or items which may be subject to legal privilege.

8.50 Where it is discovered that privileged material has been obtained inadvertently, an early assessment must be made of whether it is necessary and proportionate to retain it for one or more of the authorised purposes set out in section 122(4). If not, the material should be securely destroyed as soon as possible.

8.51 Material which has been identified as legally privileged should be clearly marked as subject to legal privilege. Such material should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes set out in section 122(4). It must be securely destroyed when its retention is no longer needed for those purposes. If such material is retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised statutory purposes.

Dissemination

8.52 Material subject to legal privilege must not be acted on or further disseminated unless a legal adviser has been consulted on the lawfulness (including the necessity and proportionality) of such action or dissemination.

8.53 The dissemination of legally privileged material to an outside body should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to remove the risk of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates, including law enforcement authorities. In this regard civil proceedings includes all legal proceedings before courts and tribunals that are not criminal in nature. Neither the Crown Prosecution Service lawyer nor any other prosecuting authority lawyer with conduct of a prosecution should have sight of any legally privileged material, held by the relevant public authority, with any possible connection to the proceedings. In respect of civil proceedings, there can be no circumstances under which it is proper for any public authority to have sight of or seek to rely on legally privileged material in order to gain a litigation advantage over another party in legal proceedings.

8.54 In order to safeguard against any risk of prejudice or accusation of abuse of process, public authorities must also take all reasonable steps to ensure that lawyers or other officials with conduct of legal proceedings should not see legally privileged material relating to those proceedings (whether the privilege is that of the other party to those proceedings or that of a third party). If such circumstances do arise, the public authority must seek independent advice from Counsel and, if there is assessed to be a risk that sight of such material could yield a litigation advantage, the direction of the Court must be sought.

Reporting to the Commissioner

8.55 In those cases where legally privileged material has been obtained via equipment interference, identified as such and then retained, the matter should be reported to the IPC as soon as reasonably practicable, as agreed with the Commissioner. Any material that is still being retained should be made available to him or her if requested, including detail of whether that material has been disseminated.

8.56 For the avoidance of doubt, the guidance in paragraphs 8.40 to 8.55 takes precedence over any contrary content of an agency's internal advice or guidance.

9 Record keeping and error reporting

Records

9.1 Records must be available for inspection by the IPC and retained to allow the Investigatory Powers Tribunal, established under Part IV of RIPA, to carry out its functions. The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates (see section 67(5) of RIPA), particularly where continuing conduct is alleged. Although records are only required to be retained for at least three years, it is therefore desirable, if possible, to retain records for up to five years. The following information relating to all 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 issuing authority or Judicial Commissioner;
- the details of what equipment interference has occurred;
- the result of periodic reviews of the warrants;
- the date of every renewal;
- the date when any instruction was given by the Judicial Commissioner to cease the equipment interference; and
- where relevant, the directions issued by the Judicial Commissioner should they refuse to approve an urgent warrant.

9.2 Records should also be kept of the arrangements by which the requirements of sections 122(3) and 177(3) (minimisation of copying and distribution of material) and sections 122(6) and 177(6) (destruction of material) are to be met.

9.3 Records should also be kept by the relevant warrant issuing department. This will include:

- All advice provided to the Secretary of State or law enforcement chief to support their consideration as to whether to issue or renew the equipment interference warrant; and
- Where the issuing of any application is not approved by the Judicial Commissioner, the grounds for refusal as given by the Judicial Commissioner and any associated advice/applications to the IPC if there is an appeal.

9.4 Each relevant equipment interference agency must also keep a record of the information below to assist the IPC in carrying out his or her statutory functions.

9.5 **Targeted warrants:** For the purposes of these record keeping requirements a targeted warrant should be taken as referring to a targeted equipment interference warrant or a targeted examination warrant, issued under part 5 of the Act. In recording this information, each relevant authority must keep a record of:

- The number of applications made by or on behalf of the equipment interference agency for a targeted equipment interference warrant;
- The number of applications for a targeted equipment interference warrant that were refused by an issuing authority;
- The number of decisions to issue a targeted equipment interference warrant that were refused by a Judicial Commissioner;
- The number of occasions that a referral was made by an issuing authority to the IPC, following the decision of a Judicial Commissioner to refuse a targeted equipment interference warrant;
- The number of targeted equipment interference warrants issued by the issuing authority and approved by a Judicial Commissioner;
- The number of targeted equipment interference warrants authorised by the issuing authority and issued by a senior official or appropriate delegate;
- The number of targeted equipment interference warrants authorised by the issuing authority and the number issued by a senior official or appropriate delegate that were subsequently refused by a Judicial Commissioner;
- The number of targeted equipment interference warrants that were renewed by the issuing authority and approved by a Judicial Commissioner;
- The number of targeted equipment interference warrants that the Judicial Commissioner refused to approve the renewal of;
- The number of targeted equipment interference warrants that were cancelled; and
- The number of targeted equipment interference warrants extant at the end of the calendar year.

9.6 For each targeted equipment interference warrant issued by the issuing authority and approved by a Judicial Commissioner (including warrants issued and approved in urgent cases), the relevant agency must also keep a record of the following:

- The statutory purpose(s) specified on the warrant;
- The details of major and minor modifications made to the warrant.

9.7 Bulk warrants:

- The number of applications made for a bulk equipment interference warrant;
- The number of applications for a bulk equipment interference warrant that were refused by a Secretary of State;
- The number of bulk equipment interference warrant that the Judicial Commissioner refused to approve the issuing of;
- The number of occasions that a referral was made by the Secretary of State to the IPC, following the decision of a Judicial Commissioner to refuse the decision to issue a bulk equipment interference warrant;
- The number of bulk equipment interference warrants issued by the Secretary of State and approved by a Judicial Commissioner;
- The number of bulk equipment interference warrants that were renewed by the issuing authority and approved by a Judicial Commissioner;
- The number of bulk equipment interference warrants that were cancelled; and
- The number of bulk equipment interference warrants extant at the end of the year.

9.8 For each bulk equipment interference warrant issued by the Secretary of State and approved by a Judicial Commissioner, the relevant agency must also keep a record of the following:

- The section 165(1)(b) purpose(s) specified on the warrant;
- The number of modifications made to add, vary or remove an operational purpose from the warrant;
- The number of modifications made to add or vary an operational purpose that were made on an urgent basis;
- The number of decisions to issue a modification to add or vary an operational purpose (including on an urgent basis) that the Judicial Commissioner did not approve;
- The number of occasions that a referral was made by the Secretary of State to the IPC, following the decision of a Judicial Commissioner to refuse to modify a bulk equipment interference warrant.

9.9 These records must be sent in written or electronic form to the IPC, as determined by him. Guidance on record keeping will be issued by the IPC. Guidance may also be sought from the Commissioner by equipment interference agencies.

Errors

9.10 This section provides information regarding errors, which are not considered to meet the threshold of a criminal or civil offence.

9.11 A relevant error which must be reported to the IPC is defined in section 209(9) of the Act as an error:

- By a implementing authority or other such persons assisting to give effect to a warrant in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner; and
- Of a description identified for this purpose in a code of practice or in guidance provided by the Commissioner.

9.12 Situations may arise where an equipment interference warrant has been obtained or modified as a result of the relevant agency having been provided with information relating to equipment – for example, by another domestic intelligence agency, police force or CSP – which later proved to be incorrect, due to an error on the part of the person providing the information, but on which the relevant agency acted in good faith. Whilst these actions do not constitute a relevant error on the part of the relevant agency, such occurrences should be brought to the attention of the Commissioner.

9.13 Proper application of the Investigatory Powers Act and thorough procedures for operating its provisions, including for example the careful preparation and checking of warrants, modifications and schedules, should reduce the scope for making errors whether by the implementing authority, CSPs or other persons assisting in giving effect to the warrant.

9.14 Any failure by the implementing authority or such other persons providing assistance to apply correctly the process set out in this code will increase the likelihood of an error occurring.

9.15 All errors described in paragraph 9.11 of this Code must be reported to the Commissioner. Errors can have very significant consequences on an affected individual's rights.

9.16 Reporting of errors will draw attention to those aspects of the equipment interference process that require further improvement to eliminate errors and the risk of undue interference with any individual's rights.

9.17 An error can only occur after equipment interference has commenced. This section of the code cannot provide an exhaustive list of possible errors. Examples could include:

- equipment interference as described in the Act has, or is believed to, have occurred without valid authorisation;
- equipment interference has taken place that would not have occurred but for conduct or an omission of the part of a member of the relevant agency or CSP;
- human error, such as incorrect transposition of equipment information from an application to a warrant or schedule which leads to the wrong material being acquired;
- warranted equipment interference has taken place on a piece of equipment but the material does not in the event relate to the intended subject where information available at the time of seeking a warrant could reasonably have indicated this;
- a material failure to adhere to the arrangements in force under section 122 of the Act relating to material obtained by targeted equipment interference, or the safeguards relating to material obtained by bulk equipment interference contained in sections 177 or 179 of the Act. For example:
  - over-collection caused by software or hardware errors;
  - unauthorised selection/examination of communications; or
  - unauthorised or incorrect disclosure of material;
  - failure to effect the cancellation of equipment interference.

9.18 When an error has been made, the implementing authority or other person which made the error (i.e. the CSP) must report the error to the Investigatory Powers Commissioner as soon as reasonably practicable after it has been established an error has occurred. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full.

9.19 If the implementing authority discovers a CSP error they should inform the Commissioner and the CSP of the error straight away to enable the CSP to investigate the cause of the error and report it themselves.

9.20 The report sent to Commissioner in relation to any error must include details of the error, the cause, the amount of material relating to the error obtained or disclosed, any unintended collateral intrusion, any analysis or action taken, whether the material has been retained or destroyed and, a summary of the steps taken to prevent recurrence. Wherever possible, technical systems should incorporate functionality to minimise errors. A senior person within that organisation must undertake a regular review of errors.

9.21 The Commissioner will keep under review the scope and nature of errors and issue guidance as necessary, including guidance on the format of error reports.

Serious errors

9.22 Section 209 of the Act states that the Commissioner must inform a person of any relevant error relating to that person which the Commissioner considers to be a serious error and that it is in the public interest for the person concerned to be informed of the error.

9.23 In circumstances where a relevant error is deemed to be of a serious nature, the Commissioner may therefore investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

9.24 If the Commissioner concludes that the error has caused significant prejudice or harm to the person concerned, the Commissioner must also decide whether he considers that it is in the public interest for the person concerned to be informed of the error. In making this decision, the Commissioner must in particular consider:

- The seriousness of the error and its effect on the person concerned; and
- the extent to which disclosing the error would be contrary to the public interest or prejudicial to:
- national security the prevention or detection of serious crime
- the economic well-being of the United Kingdom; or
- the continued discharge of the functions of any of the Security and Intelligence Agencies.

9.25 Before making its decision, the Commissioner must ask the equipment interference agency which has made the error to make submissions on the matters above.

10 Oversight

10.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints against public authority use of certain investigatory powers, including those covered by this code, as well as conduct by or on behalf of any of the intelligence agencies and is the only appropriate tribunal for human rights claims. Any complaints about the use of powers as described in this code should be directed to the IPT.

10.2 The IPC, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The IPC may undertake these inspections, as far as they relate to the IPC's statutory functions, entirely on his or her own initiative or they may be asked to investigate a specific issue by the Prime Minister

10.3 The IPC will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the IPC must not act in a way which is contrary to the public interest or jeopardise operations or investigations. All public authorities using investigatory powers must, by law, offer all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner.

10.4 Anyone working for a public authority or communications service provider who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner, who will consider them. In particular, any person who exercises the powers described in the Act or this code must, in accordance with the procedure set out in chapter 9, report to the Commissioner any action undertaken which they believe to be contrary to the provisions of this code. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority. The Commissioner may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the IPT.

10.5 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to an individual who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the individual affected. Further information on errors can be found in chapter 9 of this code. The public body who has committed the error will be able to make representations to the Commissioner before they make their decision on whether it is in the public interest for the individual to be informed. The Commissioner must also inform the affected individual of their right to apply to the Investigatory Powers Tribunal (see Complaints section for more information on how this can be done) who will be able to fully investigate the error and decide if a remedy is appropriate. The Commissioner must report annually on the findings of their inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the national interest. Only the Prime Minister will be able to authorise redactions to the Commissioner's report. If the Commissioner disagrees with the proposed redactions to his or her report then the Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

10.6 The Commissioner may also report, at any time, on any of his or her investigations and findings as they see fit. These reports will also be made publically available subject to public interest considerations. Public authorities and communications service providers may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce guidance for public authorities on how to apply and use Investigatory Powers. Wherever possible this guidance will be published in the interests of public transparency.

10.7 Further information about the IPC, their office and their work may be found at:

11 Complaints

11.1 The IPT has jurisdiction to investigate and determine complaints against public authority use of investigatory powers and human rights claims against the security and intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

11.2 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. The IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination.

11.3 This code does not cover the exercise of the Tribunal's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: www.ipt-uk.com. Alternatively information on how to make a complaint can be obtained from the following address:

The Investigatory Powers Tribunal

PO Box 33220

London

SWIH 9ZQ

11.4 If you have received a determination or decision from the IPT that you are not satisfied with then, in certain circumstances, you may have a right of appeal. The IPT will inform you when you have that right of appeal and which court you should apply to in order for your appeal application to be considered.

12 Annex A

Schedule 6: Issue of warrants under section 101 etc.

Part 1

TABLE: PART 1

Law enforcement chiefs	*Appropriate delegates*	*Appropriate law enforcement officers*
The Chief Constable of a police force maintained under section 2 of the Police Act 1996.	The person who is the appropriate deputy chief constable for the purposes of section 12A(1) of the Police Act 1996. The person holding the rank of assistant chief constable designated to act under section 12A(2) of that Act. If it is not reasonably practicable for either of those persons to act, any other person holding the rank of assistant chief constable in the force.	A member of the police force, a member of a collaborative force or a National Crime Agency officer who is included in a collaboration agreement with the police force.
The Commissioner, or an Assistant Commissioner, of the metropolitan police force.	A person holding the rank of commander in the metropolitan police force.	A member of the metropolitan police force, a member of a collaborative force or a National Crime Agency officer who is included in a collaboration agreement with the metropolitan police force.
The Commissioner of Police for the City of London.	The person authorised to act under section 25 of the City of London Police Act 1839 or, if it is not reasonably practicable for that person to act, a person holding the rank of commander in the City of London police force.	A member of the City of London police force, a member of a collaborative force or a National Crime Agency officer who is included in a collaboration agreement with the City of London police force.

The chief constable of the Police Service of Scotland.	Any deputy chief constable or assistant chief constable of the Police Service of Scotland who is designated for the purpose by the chief constable.	A constable of the Police Service of Scotland.
The Chief Constable or a Deputy Chief Constable of the Police Service of Northern Ireland.	A person holding the rank of assistant chief constable in the Police Service of Northern Ireland.	A member of the Police Service of Northern Ireland.
The Director General of the National Crime Agency.	A senior National Crime Agency Officer designated for the purpose by the Director General of the National Crime Agency.	A National Crime Agency officer or a member of a collaborative police force.
The Chief Constable of the British Transport Police.	A person holding the rank of deputy or assistant chief constable in the British Transport Police.	A member of the British Transport Police.
The Chief Constable of the Ministry of Defence Police.	A person holding the rank of deputy chief constable or assistant chief constable in the Ministry of Defence Police.	A member of the Ministry of Defence Police.
The Provost Marshal of the Royal Navy Police.	A person holding the position of deputy Provost Marshal in the Royal Navy Police.	A member of the Royal Navy Police.
The Provost Marshal of the Royal Military Police.	A person holding the position of deputy Provost Marshal in the Royal Military Police.	A member of the Royal Military Police.
The Provost Marshal of the Royal Air Force Police.	A person holding the position of deputy Provost Marshal in the Royal Air Force Police.	A member of the Royal Air Force Police.

TABLE: PART 2

Law enforcement chiefs	*Appropriate delegates*	*Appropriate law enforcement officers*
An immigration officer who is a senior official and who is designated for the purpose by the Secretary of State.	A senior official in the department of the Secretary of State by whom functions relating to immigration are exercisable who is designated for the purpose by the Secretary of State.	An immigration officer.
An officer of Revenue and Customs who is a senior official and who is designated for the purpose by the Commissioners for Her Majesty's Revenue and Customs.	An officer of Revenue and Customs who is a senior official and who is designated for the purpose by the Commissioners for Her Majesty's Revenue and Customs.	An officer of Revenue and Customs.
A designated customs official who is a senior official and who is designated for the purpose by the Secretary of State.	A designated customs official who is a senior official and who is designated for the purpose by the Secretary of State.	A designated customs official.
The Chair of the Competition and Markets Authority.	An officer of the Competition and Markets Authority designated by it for the purpose.	An officer of the Competition and Markets Authority.
The chairman or a deputy chairman, of the Independent Police Complaints Commission.	A member (other than the chair or a deputy chairman) of the Independent Police Complaints Commission who is designated by the chairman for the purpose.	A person designated under paragraph 19(2) of Schedule 3 to the Police Reform Act 2002 to take charge of, or to assist with, the investigation to which the warrant under section 100(1) relates (or would relate if issued)
The Police Investigations and Review Commissioner.	A staff officer of the Police Investigations and Review Commissioner who is designated by the Commissioner for the purpose.	A staff officer of the Police Investigations and Review Commissioner.