Home Office

DRAFT Equipment Interference Code of Practice

Pursuant to Schedule 7 to the Investigatory Powers Act 2016

February 2017

This publication is available at:
http://www.gov.uk/government/collections/investigatory-powers-bill

Any enquiries regarding this publication should be sent to us at investigatorypowers@homeoffice.gsi.gov.uk.

Contents

1 Introduction

1.1 This code of practice relates to the powers and duties conferred or imposed under Part 5 and Chapter 3 of Part 6 of the Investigatory Powers Act 2016 ("the Act"). 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. This code 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 This code of practice is primarily intended for use by the public authorities able to conduct equipment interference under the Act, namely the security and intelligence agencies (Security Service, Secret Intelligence Service ("SIS"), and Government Communications Head Quarters ("GCHQ")), law enforcement agencies (listed at Schedule 6 of the Act) and Defence Intelligence ("the equipment interference agencies"). It will also allow other interested bodies to understand the procedures to be followed by those public authorities. 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.

1.3 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 (dated January 2016) which governed the security and intelligence agencies’ use of equipment interference.

1.4 The Act provides that all codes of practice issued under Schedule 7 are admissible as evidence in criminal and civil proceedings. Any court or tribunal considering such proceedings, the Investigatory Powers Tribunal (“the IPT”), Investigatory Powers Commissioner responsible for overseeing the powers and functions conferred by the Act, or the information commissioner may take the provisions of the codes of practice 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.

1.5 Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples 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.

2 Definitions

What is equipment?

2.1 Equipment is defined in sections 135 and 19 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.

2.2 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.

What is equipment data?

2.3 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.

2.4 Equipment data is defined in sections 100 and 177 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[1].

- 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 is comprised in the communication and 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.

[1] 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.

- 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

What is protected material?

2.5 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, at the time that the selection takes place.

2.6 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[2].

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[3]. 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.

What are overseas-related communications, information and equipment data?

2.7 Overseas-related communications, overseas-related information and overseas-related equipment data are defined in section 176 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 main purpose of bulk equipment interference warrants is to obtain the communications, equipment data or other information of individuals or entities outside the British Islands.

[2] See section 193(9) of the Act.

[3] See section 193(9) of the Act.

What is a communications service provider?

2.8 The obligations under Part 5 and Chapter 3 of Part 6 of the Act apply to telecommunications operators. Throughout this code, communications service provider is used to refer to a telecommunications operator.

2.9 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, (wholly or partly) 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.

2.10 Section 261 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 and 'telecommunications system' in the Act are intentionally broad so that they remains relevant for new technologies.

2.11 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.

2.12 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 if it provides a connection to an application/website. It may also be a telecommunications operator if and in so far as it provides a messaging service.

2.13 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.

3 Scope of equipment interference

3.1 This chapter provides background on equipment interference and guidance on the scope of the equipment interference provisions in the Act, setting out the circumstances where an equipment interference warrant is mandatory. It also details circumstances where an equipment interference warrant may be applied for and clarifies when the provisions of the Act are not applicable.

Equipment interference capabilities

3.2 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 equipment. Equipment interference can be carried out either remotely or by physically interacting with the equipment.

3.3 Equipment interference operations vary in complexity. At the lower end of the complexity 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.

Restrictions on interference with equipment

Human Rights Act 1998

3.4 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.

3.5 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, the right to peaceful enjoyment of possessions, which could include any equipment subject to interference.

Computer Misuse Act 1990

3.6 The use of equipment interference techniques may also necessarily involve interference with computers. 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.

3.7 "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 derived from the courts' interpretation of "computer" as used in 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 135 and 198 of the Act.

3.8 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.

3.9 Where an equipment interference agency has obtained an appropriate authorisation no offence will be committed by virtue of the CMA.

Equipment interference warrants

3.10 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. Conduct which has lawful authority by virtue of an equipment interference warrant is treated as lawful for all other purposes. Further detail on the types of equipment interference warrants, the relevant processes and considerations is provided at Chapters 4 to 6 of this code.

3.11 Equipment interference warrants authorise interference with any equipment for the purpose of obtaining communications, equipment data or other information. 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).

3.12 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 live communications[4] (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. An equipment interference warrant may however authorise the acquisition of communications that are stored by or on equipment.

3.13 The material obtained under an equipment interference warrant may be used evidentially or as intelligence. In the case of an equipment interference warrant authorising testing, training, maintenance or development the material so obtained may only be used for this purpose. Further detail on handling and retention of material acquired by equipment interference is provided at Chapter 9 of this code.

Incidental conduct

3.14 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). 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.

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

3.15 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 is unexpectedly exposed to two devices, and cannot determine which is the target device without conducting preliminary examinations. The agency is permitted to examine both devices using equipment interference techniques in order to clarify which one belongs to the target – this is incidental conduct, which may involve the obtaining of data from the other device. For the device not connected to the target, the full equipment interference described in the warrant will not take place and any data already obtained relating to that device will be deleted as soon as possible.

3.16 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.

Surveillance

3.17 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).

3.18 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 surveillance will be considered as part of the equipment interference authorisation.

3.19 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.

3.20 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.

3.21 For example, if an equipment interference agency wishes to conduct separate surveillance by directing an officer to observe 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 5.96 onwards).

Interception

3.22 An equipment interference warrant cannot authorise conduct that would amount to an offence, under section 3(1) of the Act, of intentional interception of a communication in the course of its transmission (e.g. live interception of an online video call) except if the person has a right to control the operation or use of the system, or has the express or implied consent of such a person to carry out the interception. If conduct proposed by an equipment interference agency amounts to the interception live communications[5] an interception warrant under Part 2 or Chapter 1 of Part 6 of the Act would be required. Interception warrants may be sought by the head of an intelligence service, the Director General of the NCA, the Commissioner of the Metropolitan Police Service, the Chief Constable of the Police Service of Northern Ireland, the Chief Constable of the Police Service of Scotland, the Commissioners for Her Majesty's Revenue & Customs and the Chief of Defence Intelligence. 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 of the video calls in the course of their transmission cannot be authorised by an equipment interference warrant as incidental conduct. An interception and equipment interference warrant must both be obtained (either as a combined warrant or separately).

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

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

3.23 Section 13 of the Act provides that it is mandatory for a security and intelligence agency agencies (referred to in the Act as an "intelligence service") to obtain an equipment interference warrant for the purpose of obtaining communications, private information or equipment data where a CMA offence would otherwise be committed and there is a British Islands connection.

3.24 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 security and intelligence agency 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: 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.

3.25 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 chapter 6 of this code.

Law enforcement agencies - Further restrictions on interference with equipment

3.26 The Act provides a statutory framework under which law enforcement agencies may authorise targeted equipment interference. 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.

3.27 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 section 93 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 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). There are a number of statutes that are used for the purpose of obtaining material (including communications and private information) for evidential purposes. Those that are most commonly used by law enforcement agencies to access or obtain material include (but are not limited to) the following:

- Powers to search, seizure or production under the Police and Criminal Evidence Act 1984
- Powers to search or obtain material under the Proceeds of Crime Act 2002
- Powers to search under the Firearms Act 1968, Protection of Children Act 1978, Theft Act 1968 and the Misuse of Drugs Act 1971
- Powers to examine imported goods under the Customs and Excise Management Act 1979 to examine imported goods
- Powers to examine material under Schedule 7 of the Terrorism Act 2000

Example: A law enforcement officer interferes with equipment to obtain information stored in electronic form on that equipment under his powers of seizure 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.

3.28 Section 107 places restrictions on the issue of equipment interference warrants to specified law enforcement agencies. 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 the law enforcement chief considers there is a British Islands connection. A British Islands connection exists if:

- any of the conduct authorised by the warrant would take place in the British Islands (regardless of the location of the equipment that would, or may, be interfered with),
- any of the equipment which would, or may, be interfered with 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—

  a) communications sent by, or to, a person who is, or whom the law enforcement officer believes to be, for the time being in the British Islands,

  b) information relating to an individual who is, or whom the law enforcement officer believes to be, for the time being in the British Islands, or

  c) equipment data which forms part of, or is connected with, communications or information falling within (a) or (b).

3.29 To further ensure that equipment interference activities conducted by these agencies are focussed on investigations or operations within the British Islands, irrespective of whether there is a British Islands connection, they 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 as per section 107 (4) of the Act.

Example: A law enforcement agency has obtained an equipment interference warrant authorising the acquisition of communications, equipment data and other information 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.

3.30 Law enforcement agencies other than those set out in section 107(2) of the Act may be issued with targeted equipment interference warrants regardless of whether there is a British Islands connection. Officers in these agencies 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

3.31 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.

3.32 First, an equipment interference warrant is not mandatory where the conduct in question would not be an offence under the CMA. As an example, an equipment interference agency may obtain the informed consent of a person able to give permission in respect of the interference with the relevant equipment, thus making it authorised[6].

Example: An equipment interference agency gains access to a company's computer server with their informed consent in order to test the company's protections against cyber-attacks. As this access is not unauthorised, the interference does not amount to an offence under the CMA and so an equipment interference warrant is not required.

3.33 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.

[6] Offences under the CMA are dependent upon "unauthorised" access to computer material being obtained. Sections 17(5) and 17(8) of the CMA provide further explanation of the meaning of "unauthorised" in this context.

3.34 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 agency 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.

3.35 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 9 of this code.

Ministry of Defence

3.36 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).

Property interference

3.37 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. Interference with equipment that is not for the purpose of acquiring communications, equipment data or other information will continue to constitute 'property interference' and be capable of authorisation under section 5 or 7 of Intelligence Services Act 1994 ("the 1994 Act") or Part 3 of the Police Act 1997 ("the 1997 Act"). The Covert Surveillance and Property Interference Code of Practice sets out the relevant considerations and safeguards that apply to property interference.

3.38 Applicants therefore need to consider not only whether they will be obtaining communications, equipment data or other information when they interfere with equipment, but also whether this is the purpose of the interference. If the acquisition of communications, equipment data or other information is incidental and not the purpose of the interference, then this activity should continue to be authorised as property interference.

3.39 For example, an equipment interference agency recognises that the process by which it disables a particular CCTV camera results in it obtaining a stored copy of footage from the CCTV system. In such circumstances, although the agency is interfering with equipment (the CCTV system) and acquiring communications and/or private information, the purpose of the interference is to disable the CCTV camera. The acquisition of the CCTV footage is intended, in so far as it is a constituent part of the interference required to disable the CCTV camera, but is entirely incidental. Accordingly, this activity can continue to be authorised as property interference under the 1994 Act or 1997 Act (as applicable).

3.40 This can be contrasted with where an equipment interference agency is seeking to monitor the movements of a target who has been captured on CCTV footage. In such circumstances, the equipment interference agency interferes with the CCTV system for the purpose of acquiring a copy of the footage; the purpose of the interference with the equipment is to acquire communications and/or private information and an equipment interference warrant would be required.

3.41 The Act applies 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 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 and the Covert Surveillance and Property Interference Codes of Practice.

4 Warranted equipment interference – general rules

4.1 A targeted equipment interference warrant under Part 5 or a bulk equipment interference warrant under Chapter 3 of Part 6 of the Act will provide a lawful basis for an equipment interference agency to carry out equipment interference for the purposes of obtaining communications, equipment data or other information.

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

4.3 .In no circumstances may an equipment interference agency ask any international partner to undertake equipment interference on its behalf where the making of the request would amount to a deliberate circumvention of the Act. Such requests will not amount to deliberate circumvention where, for example, the equipment interference agency does not have the required access to a piece or multiple pieces of equipment and it is not therefore technically feasible for the equipment interference agency to obtain the data under the Act.

Types of warrants

4.4 Part 5 of the Act provides for targeted equipment interference warrants and examination warrants - further guidance on these warrants is set out in Chapter 5 of this code. In addition, Part 3 of Chapter 6 of the Act provides for bulk equipment interference warrants, further guidance on which is set out in Chapter 6 of this Code.

- A **targeted equipment interference warrant** (see section 99 (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. Such a warrant will also authorise any conduct it is necessary to undertake to do what is expressly authorised or required by the warrant.

- A **targeted examination warrant** (see section 99(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 193(4) of the Act. This type of warrant must be sought in all cases where protected material is to be selected for examination on the basis of criteria referable to an individual who the person making the request knows to be in the British Islands at the time that the content is selected for examination.

- A **bulk equipment interference warrant** (see section 176 of the Act) is a warrant which has as its main purpose the obtaining of overseas-related communications,

equipment data and other information, and which authorises the acquisition of communications, equipment data and other information and/or the selection for examination of the communications, equipment data and other information. A bulk equipment interference warrant will also authorise any conduct it is necessary to undertake to do what is expressly authorised by the warrant.

Equipment interference agencies

4.5 There are a limited number of persons who can make an application for an equipment interference warrant, or on whose behalf an application can be made on as set out at sections 102 to 104 and 106. These are:

- The Director General of the Security Service,
- The Chief of the Secret Intelligence Service,
- The Director of the Government Communications Headquarters (GCHQ),
- The Chief of Defence Intelligence,
- The Chief Constable of a police force maintained under section 2 of the Police Act 1996,
- The Commissioner, or an Assistant Commissioner, of the metropolitan police force,
- The Commissioner of Police for the City of London,
- The chief constable of the Police Service of Scotland,
- The Director General of the National Crime Agency,
- The Chief Constable of the British Transport Police Force,
- The Chief Constable or a Deputy Chief Constable of the Police Service of Northern Ireland,
- The Chief Constable of the Ministry of Defence Police,
- The Provost Marshal of the Royal Navy Police,
- The Provost Marshal of the Royal Military Police,
- The Provost Marshal of the Royal Air Force Police,
- An immigration officer who is a senior official and who is designated for the purposes by the Secretary of State,

- An officer of Revenue and Customs who is a senior official and who is designated for the purpose by the Commissioner for Her Majesty's Revenue and Customs,
- A designated customs official who is a senior official and who is designated for the purpose by the Secretary of State,
- The Chair of the Competition and Markets Authority,
- The chairman, or a deputy chairman, of the Independent Police Complaints Commission, and
- The Police and Investigations and Review Commissioner.

4.6 In the case of bulk equipment interference warrants, the only persons who can make an application, or on whose behalf an application can be made, are:

- The Director General of the Security Service.
- The Chief of the Secret Intelligence Service.
- The Director of the Government Communications Headquarters (GCHQ).

4.7 For the purposes of the Act and this code of practice, the Service Police (Royal Navy Police, Royal Military Police and Royal Air Force Police) and the Ministry of Defence Police, are considered separate authorities to the Ministry of Defence.

4.8 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 a relevant law enforcement officer, listed in Schedule 6 of the Act.

Necessity and proportionality

4.9 Equipment interference is likely to involve an interference with a person's rights under the ECHR. This is only justifiable if the interference is necessary for a legitimate purpose and proportionate to that purpose. The Act recognises this by first requiring that the issuing authority considers that the warrant is necessary for one or more of the following statutory grounds set out in section 20 of the Act: Applications for targeted equipment interference warrants and examination warrants may be made by or on behalf of the head of a security and intelligence agency:

- In the interests of national security;
- For the purpose of preventing or detecting serious crime; serious crime is defined in section 263(1) as crime where the offence is one 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;

- 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. The power to issue an 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 and Judicial Commissioner 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. The power to issue an equipment interference warrant for the purpose of safeguarding the economic well-being of the UK may 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.

4.10 Applications for targeted equipment interference warrants may be made by or on behalf of the Chief of Defence Intelligence in the interests of national security;

4.11 Applications for targeted equipment interference warrants may be made by an appropriate law enforcement officer in the interests of preventing or detecting serious crime. For certain law enforcement agencies, applications may also be made for a warrant on the grounds 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. Only law enforcement agencies listed in Part 1 of Schedule 6 of the Act may apply for a warrant for this purpose. 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.

4.12 Some law enforcement agencies may only carry out equipment interference for the purpose of preventing or detecting serious crime and when in relation to specific functions of that 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.

- For the Independent Police Complaints Commission, the offence, or all of the offences, to which the serious crime relates are offences that are being investigated as part of an investigation by the Commission under Schedule 3 to the Police Reform Act 2002.

- For the Police Investigations and Review Commissioner, the offence, or all of the offences, to which the serious crime relates are offences that are being investigated as part of an investigation by the Commission under 33A (b)(i) of the Police, Public Order and Criminal Justice (Scotland) Act 2006.

4.13 Applications for bulk equipment interference warrants may only be made by or on behalf of the head of a security and intelligence agency in the interests of national security, for the purpose of preventing or detecting serious crime and in the interests of economic wellbeing. At least one of the grounds for issuing a bulk equipment interference warrant must always be national security.

4.14 The issuing authority must also believe that the conduct authorised 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 interference with the 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 conduct authorised should bring an expected benefit and should not be disproportionate or arbitrary.

4.15 Section 2 of the Act requires the public authority to have regard to the following when issuing, renewing, modifying or cancelling a warrant under Part 5 or 6:

- whether what is sought to be achieved could reasonably be achieved by other less intrusive means,

- whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant is higher because of the particular sensitivity of that information. This includes whether additional safeguards (as set out in Chapter 9) should apply and whether threshold for the conduct to be proportionate is higher because of the sensitivity of the information,

- 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 (including the obligation for a public authority to comply with the Human Rights Act).

4.16 In the case of warrants issued under sections 101(1)(g) and (h) and (2)(d) and (e) of the Act for the purposes of testing, maintenance, development or training, proportionality should be considered by assessing the potential for, and seriousness of, intrusion into any affected persons' privacy and interference with property against the benefits of carrying out the proposed exercise. The issuing authority must be clear that it is also required for at least one of the relevant statutory purposes.

4.17 No interference should be considered proportionate if the material which is sought could reasonably be obtained by other less intrusive means.

4.18 The following elements of proportionality should therefore be considered:

- The extent of the proposed interference with privacy against what is sought to be achieved;
- how and why the methods to be adopted will cause the least possible interference on to the subject and others;
- whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- what other methods, as appropriate, were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the use of the proposed investigatory power;
- 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;
- where a bulk equipment interference warrant is available, the safeguards set out in Chapter 3 of Part 6 of the Act.

Trade Unions

4.19 As set out in sections 102 to 104 and 106 the fact that the information that would be obtained under the 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, for example, 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 users of equipment and systems

4.20 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 likelihood or severity of any unauthorised intrusion into the privacy; or increase in the 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.

4.21 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.

4.22 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 4.21In 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.

5 Targeted warrants

5.1 This section applies to the two kinds of warrants that may be issued under Part 5 of the Act (as set out at paragraph 4.4). 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).

5.2 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. The role of the Judicial Commissioner in approving the decision to issue warrants is explained in paragraph 5.55. Prior to submission to the issuing authority, each application should be subject to a review within the agency seeking the warrant. This review involves scrutiny by more than one official, who will consider whether the application is for a purpose falling within section 102, 103, 104 or 106 of the Act and whether the interference proposed is both necessary and proportionate. A copy of each warrant application should be retained by the equipment interference agency.

5.3 Although a warrant will be applied for by one of the equipment interference agencies, this does not prevent another agency assisting them with giving effect to the warrant.

5.4 In the case of the **security and intelligence agencies**, warrants may be issued by the Secretary of State on an application made by or on behalf of the head of a security and intelligence agency. 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, a warrant may be issued by a Scottish Minister.

5.5 In the case of **defence intelligence**, warrants may be issued by the Secretary of State on an application made by or on behalf of the chief of Defence Intelligence.

5.6 In the case of **law enforcement agencies**, 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.

Subject-matter of targeted warrants

5.7 Section 101 sets out the subject-matter of targeted warrants and constrains what equipment can be described in the warrant or what material can be selected for examination. The subject-matter of equipment interference and examination warrants may be targeted or thematic.

Targeted warrants relating to a person, organisation or particular location

5.8 In many cases, equipment interference and examination warrants will relate to subjects as set out in sections 101(1)(a) and (d). Section 101(1)(a) and (d) warrants are sometimes referred to as "non-thematic" warrants and may relate to one or a combination of:

- equipment belonging to, used by or in the possession of a particular person;
- equipment belonging to, used by or in the possession of a particular organisation; or
- equipment in a particular location.

5.9 A "person" for these purposes may be an individual but, as defined in the Interpretation Act 1978, a person also includes a body of persons corporate or unincorporate[7]. An "organisation" may additionally include entities that are not legal persons. This means, for example, that a warrant may relate to a particular company. In such a case, the company is the "person" to which the warrant relates (e.g. the focus of the warrant is the company itself) and section 115(3) will not impose an obligation to name individual employees or workers in the warrant, 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.

5.10 In practice, an equipment interference agency may need to build intelligence about the legal person or organisation itself, rather than the individuals who are directors, employees or members of the company or organisation. In such circumstances, it may be more appropriate to obtain a warrant against e.g. a company, as opposed to individuals working for it. However, in certain circumstances, such as where a warrant is against a large organisation, the intrusion may be higher than a warrant targeting a small subset of individuals working for that organisation. As such, the equipment interference agency will need to justify why it is necessary and proportionate to target the company itself, rather than a limited number of individuals working for that company. 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 and their identities will not be known (or could only be ascertained by further interferences with privacy). Individual names are not required to ascertain the scope of the warrant or the interference with privacy authorised.

[7] See Schedule 1 to the Interpretation Act 1978.

5.11 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. Equipment interference 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

5.12 In other cases, Part 5 warrants will relate to equipment linked by a common theme. 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. Thematic warrants, as set out at sections 101(1)(b), (c) and (e) to (h) and 101(2)(b) to (e) of the Act, may relate to:

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.

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

c. equipment in more than one location, where the interference is for the purpose of a single investigation or operation.

d. equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description

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

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.

5.13 A thematic warrant may be appropriate where the proposed activity is most suitably dealt with by a thematic subject-matter, where the relevant statutory tests are met and where the use of a series of individual warrants, adds no benefit in terms of accountability and oversight.

Specificity of thematic warrants

5.14 The Act requires that certain additional details must be included in the warrant dependent on the subject-matter(s) of the warrant[8]. For example, a thematic warrant that relates to equipment used by a group which shares a common purpose must include a description of that purpose as well as the name or description of as many of the persons who form part of that group as it is reasonably practicable to name or describe. An equipment interference agency must, when section 115 requires, name or describe as many of the persons, organisations, or locations as is reasonably practicable at the time of the application. The descriptions of persons, organisations, or locations provided in a warrant application must be as granular as reasonably practicable in order to sufficiently enable proper assessment of the proportionality and intrusion involved in the interference. In some cases aliases may be used in place of names or descriptions, for example where their real name is not known.

5.15 However, it may not always be reasonably practicable to include the names or descriptions of each and every one of the persons, organisations or locations. Accordingly thematic warrants can be seen to fall into two types, those where it is reasonably practicable to include additional details and those where it is not:

[8] As per section 115(3) and 115(5).

Example of interference where it is reasonably practicable to include additional details of those falling within the subject-matter of the warrant: An equipment interference agency wishes to interfere with the equipment of people for the purposes of an investigation in to human trafficking. The agency applies for a warrant in relation to "equipment used by more than one person for the purpose of operation X" and three of those persons are known to be ''Mr A', 'Mr B' and 'Mrs C''. As it is reasonably practicable to do so their names must be included in the warrant at the point of issuing. Once issued, this warrant authorises interference with the equipment used by ''Mr A', 'Mr B' and 'Mrs C'', the type of equipment must be described within the warrant in accordance with section 115(4), Further equipment or further names must be added by modification (see paragraph 5.21) if the agency wishes to undertake further activity.

Example of interference where it is not reasonably practicable to include additional subject-matter details: An equipment interference agency wishes to identify persons accessing terrorist material online. The agency seeks a thematic warrant in relation to more than one person carrying on a particular activity, with the subject-matter of the warrant being "equipment used by persons be accessing the terrorist website 'X'". In such a case, it may not be reasonably practicable to name or describe those persons any further than by a description which is based on their use of website 'X'. Once issued the subject-matter of this warrant is equipment used by persons known to be accessing the terrorist website 'X' and the authorised interference with any type of equipment described in the warrant falling in to that description is lawful. There is no requirement to modify the warrant in accordance with section 115(3) to add names or descriptions of persons accessing the website.

5.16 In the case of the second example, the requirements of the Act would be met as the warrant describes the persons, as far as is reasonably practicable, by reference to them accessing the relevant website. However the warrant application must make clear why the subject-matter is appropriate, and why it is not reasonably practicable to name or describe any further those falling within the relevant subject-matter. There is no requirement to modify warrants falling into this category during the currency of the warrant providing any additional names or descriptions already fall within the subject-matter of the warrant and the description of the persons.

5.17 The practicability of providing individual names or descriptions will need to be assessed on a case by case basis by the equipment interference agency making the application and will depend upon, for example, the existing intelligence picture, the scale and pace of the operation, the nature of the equipment to be interfered with and the time constraints of the particular operation.

5.18 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.

Authorisation of thematic warrants

5.19 Before issuing a thematic warrant the issuing authority must be satisfied that it is necessary and proportionate to issue it and that the subject matter and the method of naming or describing the additional details provided in relation to the subject matter are compliant with the requirements of section 115(3) or 115(5) of the Act.

5.20 The thematic warrant application, including the necessity and proportionality of the proposed conduct, the assessment of collateral intrusion, and the further details provided in relation to the subject-matter of the warrant are provided to assist the issuing authority and judicial commissioner in foreseeing the extent of the interference with privacy to be authorised by the warrant. The issuing authority's foresight of the interference with privacy has to be sufficient to allow them to make a proper decision as to the necessity and proportionality of the conduct authorised; otherwise the warrant should not be issued.

Modification of thematic equipment interference warrants

5.21 Thematic equipment interference warrants may be modified subject to the provisions in the Act (further detail on modifications, including how they apply to non-thematic warrants, is set out at paragraphs 5.73 to 5.92)

5.22 The modifications that can be made to a thematic equipment interference warrant are:

- Adding or removing a matter to which the warrant relates;
- Adding, varying or removing a name or description in relation to a subject-matter; or,
- Adding, varying or removing a description of the type of equipment to be interfered with.

5.23 The ability to modify the names or descriptions apply only to thematic warrants[9]. The requirement to modify these details varies depending on the subject-matter of the original warrant and whether the warrant does or does not provide additional names or descriptions of the persons, organisations or locations in relation to the subject-matter (as illustrated in the examples in paragraph 5.15).

[9] See section 118(3).

5.24 For example, for thematic equipment interference warrants which specifically name or describe every person, organisation or location individually, modifications must be made to add, vary or remove any names or descriptions. Modifications will also be required where the equipment interference agency wishes to interfere with a type of equipment that was not originally described in the warrant.

5.25 Where a thematic equipment interference warrant does not individually name or describe additional persons, organisations or locations, but either describes the thematic subject-matter alone, or provides general descriptions within the subject-matter (for example 'the media wing of an overseas terrorist organisation'), modifications are not required to interfere with the equipment of any additional person, organisation or equipment in any location as long as one of these conditions is met:

- Where it has not been reasonably practicable to provide any additional details, the persons organisations or locations fall within the thematic subject-matter; or

- where it has been reasonably practicable to provide details in the form of general descriptions falling within the subject matter, the persons, organisations or locations fall within one of those general descriptions.

5.26 Modifications to add individual names or descriptions are not necessary in these circumstances as the warrant already provides lawful authority to interfere with the equipment within the subject-matter, or within any of the general descriptions falling within the subject matter that may have been provided. As described in paragraph 5.19, the issuing authority must consider the authorised conduct to be necessary and proportionate before issuing the warrant and must clearly understand the extent of the interference that they are authorising.

5.27 If, over the course of an operation, an equipment interference agency considers that the nature of the operation has developed in such a way that the authorised activity might not be considered necessary and/or proportionate, they must consider whether the warrant should be modified pursuant to the requirement to ensure that any warrant remains necessary and proportionate. If the agency determines the warrant is no longer necessary and proportionate, even if modified, then it must be cancelled.

5.28 There is an on-going duty to review warrants and to cancel them if they are no longer considered to be necessary and proportionate. More detail regarding the cancellation of warrants can be found in paragraph 5.93.

Example: An equipment interference agency may seek a warrant to interfere with the equipment of group of persons known to meet regularly and they need to be rapidly investigated because intelligence suggests they are involved in activities threatening national security. The agency sets out in the application that they will be unable to individually name or describe the people within this group in advance due to the speed of the work. However, over the course of the operation, the agency determines that only a proportion of people falling within the description of the group are of intelligence interest. The equipment interference agency must assess whether the proportionality case put to and accepted by the issuing authority and the Judicial Commissioner remains accurate or need to be narrowed. If the change in circumstances affects the proportionality of the warranted activity then the warrant may need to be modified to reflect more precisely those subject to interference or the issuing authority should be notified that the warrant may need to be cancelled.

Renewal of thematic warrants

5.29 The provisions relating to renewal of warrants, described further in paragraph X, apply to thematic warrants. An agency seeking to renew a thematic warrant must present in the renewal application a thorough assessment of the proportionality of conduct to date, including any collateral intrusion, and the extent of any interference with privacy. In particular, when seeking to renew a thematic warrant that does not specifically name or describe each person, organisation or location, the applicant should explain how the warrant continues to meet the requirements of section 115(3) or 115(5). The renewal application should provide any further, relevant information about those who fall within the subject-matter of the warrant and, if relevant, the additional details provided in order to sufficiently enable assessment of the intrusion involved in the activity authorised. This information will ensure that the issuing authority and Judicial Commissioner will have further opportunity to consider the necessity and proportionality of the interference, supported by up to date information.

Consideration of bulk equipment interference warrants

5.30 If the issuing authority is (a) 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, (b) can therefore properly and fully assess necessity and proportionality, and (c) agrees that it is necessary and proportionate, then a thematic warrant may 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.

Example: 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. .

Example: Intelligence suggests that a terrorist cell dispersed across a small number of locations in the Middle East is plotting an imminent bomb attack against UK interests. 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.*

Format of warrant application

Targeted equipment interference warrants

5.31 In this chapter, reference to an 'application' for a warrant includes the application form and the draft warrant (including the draft instrument and any draft schedules). An application for a targeted equipment interference warrant, a copy of which must be retained by the applicant, should contain the following information:

a. The statutory ground(s) for which the issue of the warrant is considered necessary. 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;

b. 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;

c. 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, describe the purposes of the activity and 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;

d. A description of any communications, equipment data or other information that is to be (or may be) obtained and an outline of how obtaining the material will benefit the investigation or operation;

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 expected will be 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. Consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, including whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means;

i. Where a thematic equipment interference warrant either lists the subject-matter alone, or provides additional details by means of general descriptions rather than individual names or descriptions, the warrant application should say why it is not reasonably practicable to individually name or describe persons, organisations or sets of locations 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 4.18);

j. What measures will be put in place to ensure proportionality is maintained (for example, any 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);

k. 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;

l. Where the warrant is likely to result in the obtaining of legally privileged material, a statement to that effect, an assessment of how likely it is that such material will be included and what protections it is proposed will be applied to the handling of information so obtained;

m. Where the purpose, or one of the purposes, of the warrant is to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege, a statement to that effect and an assessment of why there are exceptional and compelling circumstances that make the acquisition of such items necessary and what protections it is proposed will be applied to the handling of the information so obtained;

n. if the intention is to obtain items that would be subject to legal privilege if the material were not created or held with the intention of furthering a criminal purpose, the application should contain a statement to that effect and set out the reasons for believing that the material will be created or held with the intention to further a criminal purpose;

o. Where the purpose of the warrant is to obtain communications or private information of a member of a relevant legislature (as defined in section 111) (see Chapter 9), a statement to that effect and what protections it is proposed will be applied to the handling of the information so obtained;

p. Where the warrant is intended to authorise or require interference with equipment for the purpose of obtaining communications or other items of information which the applicant believes will contain confidential journalistic material or to identify or confirm the source of journalistic information, a statement to that effect and what protections it is proposed will be applied to the handling of the information so obtained;

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

r. An assurance that all material obtained will be kept for no longer than necessary and handled in accordance with the safeguards required by section 129 of the Act and chapter 9 of this code.

5.32 When completing a warrant application, the agency must ensure that the case for the warrant is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which support or weakens the case for the warrant.

Targeted examination warrants

5.33 A **targeted examination warrant** described in section 99(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 193(4) of the Act, of protected material obtained under a bulk equipment interference warrant of an individual known at that time to be in the British Islands.

5.34 Targeted examination warrants may be issued by the Secretary of State or where relevant the Scottish Ministers on an application made by or on behalf of the head of a security and intelligence agency. An application for a targeted examination warrant, a copy of which must be retained by the applicant, contain the following information:

a. The statutory ground(s) for which the issue of the warrant is considered necessary, as set out in section 102(3) or 103(2);

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

c. 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 describe the common purpose or activity, and 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, maintenance, development and/or training activities must describe the nature of the testing, maintenance or development of capabilities and/or a description of the training.

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

e. Consideration of why the selection for examination to be authorised by the warrant is proportionate to what is sought to be achieved, including whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means;

f. Where a thematic examination warrant either lists the subject-matter alone, or provides additional details by means of general descriptions rather than individual names or descriptions, the warrant application should say why it is not reasonably practicable to individually name or describe persons, or organisations Consideration of any collateral intrusion and why that intrusion is justified in the circumstances;

g. Where the purpose, or one of the purposes, of the warrant is to examine items subject to legal privilege, a statement to that effect and an assessment of why there are exceptional and compelling circumstances that make the examination of such items necessary and what protections it is proposed will be applied to the handling of the information so obtained;

h. Where it is considered likely that legally privileged items will be included in the material to be examined, a statement to that effect and an assessment of how likely it is that such items will be included in the material and what protections it is proposed will be applied to the handling of information so obtained;

i. If the intention is to select for examination items that would be subject to legal privilege if the items were not created or held with the intention of furthering a criminal purpose, the application should contain a statement to that effect and set out the reasons for believing that the items are created or held with the intention to further a criminal purpose;

j. Where the purpose of the warrant is to examine communications or private communication of a member of a relevant legislature (as defined in section 111) (see Chapter 9), a statement to that effect and what protections it is proposed will be applied to the handling of the information so obtained;

k. Where the warrant is intended to authorise the selection for examination of material which the application believes is confidential journalistic material or to identify or confirm the source of journalistic information, a statement to that effect and what protections it is proposed will be applied to the handling of the information so obtained;

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

m. 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 129 of the Act (see chapter 9).

5.35 When completing a warrant application, the agency must ensure that the case for the warrant is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which support or weakens the case for the warrant.

Format of Part 5 warrants

5.36 A targeted equipment interference 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. Part 5 warrants must include the details specified in the second column of the relevant table in section 115 (3) of the Act that relate to the subject matter described in the first column.

5.37 Targeted equipment interference warrants or targeted examination warrants, when issued to the security and intelligence agencies, are addressed to the head of the intelligence service by whom or on whose behalf the application for the warrant was made. In the case of the Ministry of Defence, warrants are addressed to the Chief of Defence Intelligence.

5.38 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 officer who is accountable for giving effect to the warrant (who may or may not be the applicant)

5.39 Where required, (for example because of uncertainty over real identity) names or descriptions on the warrant can be in the form of an alias or other description that identifies the subject.

Targeted equipment interference warrants

5.40 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 will include the following information:

- A statement that it is a targeted equipment interference warrant;
- The person to whom it is addressed;

- A warrant for equipment that relates to a particular person or organisation or to a particular location must name or describe that person or organisation or the location;
- A warrant for equipment that relates to a group of persons who share a common purpose or who carry on (or who may carry on) a particular activity must describe that purpose or activity, and name or describe as many of those persons as it is reasonably practicable to name or describe;
- Where the warrant for equipment that relates to more than one person, organisation or location, and where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation it should describe the nature of the investigation or operation and name or describe as many of those persons or organisations, or as many of the locations as it is reasonably practicable to name or describe;
- A warrant for equipment being used for a particular activity or activities must describe those activities;
- A warrant that relates to any testing, training activities, maintenance or the development of capabilities must describe the nature of the testing, training, maintenance or development of those capabilities.;
- Date the warrant was issued;
- A warrant reference number.

5.41 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 132 of the Act. This may include, for example, disclosure of material for admission as evidence in criminal and civil proceedings.

Targeted examination warrants

5.42 Each targeted examination warrant will comprise a warrant instrument signed by the Secretary of State and may also include a schedule or set of schedules.

5.43 The warrant will include:

- A statement that it is a targeted examination warrant;
- The person to whom it is addressed;
- 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 who may carry on) a particular activity must describe that purpose or activity, and

name or describe as many of those persons as it is reasonably practicable to name or describe;

- Where the warrant relates to more than one person or organisation, and where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation it should describe the investigation or operation and name or describe as many of those persons or organisations, as it is reasonably practicable to name or describe;
- A warrant that relates to any testing or training activities must describe those activities;
- Date the warrant was issued;
- A warrant reference number.

Authorisation of a targeted equipment interference warrant

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

a. The warrant is necessary in the case of security and intelligence agencies for the purposes described in paragraph 4.9;

b. The warrant is necessary in the case of Defence Intelligence for the purposes described in 4.10;

c. The warrant is necessary in the case of law enforcement agencies: for the purposes described in 4.11;

d. 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;

e. There are satisfactory safeguards in place. The issuing authority must consider that satisfactory arrangements are in force in relation to the warrant. These safeguards relate to the copying, dissemination, retention of material obtained by equipment interference and are explained in Chapter 9 of this code;

f. The Secretary of State has received approval from the Prime Minister where the additional protection for members of a relevant legislatures applies (see section 111 of the Act or paragraph 9.36 of the code of practice);

g. The issuing authority is satisfied that there are exceptional and compelling circumstances where the purpose, or one of the purposes, of the warrant is to obtain or examine items subject to legal privilege;

h. The issuing authority is satisfied that specific arrangements are in place for the handling, retention, use and destruction of items subject to legal privilege where the warrant is likely to result in the acquisition or examination of such items;

i. Where the purpose, or one of the purposes, of the warrant is to obtain material containing confidential journalistic information or to identify or confirm a source of journalistic information, the issuing authority is satisfied that specific arrangements are in place for the handling, retention, use and destruction of such material;

j. The issuing authority has complied with Section 2 of the Act, which imposes general duties in relation to privacy. The issuing authority must consider: whether what is sought to be achieved by the warrant could be achieved by less intrusive means; whether the level of protection to be applied to information obtained under the warrant is higher because of the particular sensitivity of that information; the public interest in the integrity and security of telecommunications systems and postal services; and any other aspects in the public interest in the protection of privacy;

k. 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 108 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.

Power of Scottish Ministers to issue warrants

5.45 Part 5 warrants may be issued by the Scottish Ministers to the security and intelligence agencies for the purposes of the prevention and detection of serious crime. The functions of the Scottish ministers also cover renewal, modification and cancellation arrangements. Sections 103 of the Act makes sets out the circumstances in which the Scottish Ministers may issue such warrants. A targeted equipment interference warrant may only be issued by the Scottish Minister if the equipment is, or believed to be, in Scotland at the time of issue. A targeted examination warrant may only be issued if it would relate only to a person that is, or believed to be, in Scotland at the time of the issue of the warrant.

Authorisation of a Part 5 warrant: senior official signature

5.46 The Act permits that when it is not reasonably practicable for the Secretary of State or member of the Scottish Government to sign Part 5 warrant a delegate may sign the warrant on their behalf. Typically this scenario will arise where the 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 or member of the Scottish Government must still personally authorise the conduct authorised by the warrant. When seeking authorisation the senior official must explain the case, either in writing or orally, to the Secretary of State or member of the Scottish Government and this explanation should cover the considerations and information that would be included on an application form as set out at paragraph 5.31. This will include an explanation of necessity and proportionality. Once authorisation has been granted the warrant may be signed by a senior official. If the Secretary of State or member of the Scottish Government 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. Except in urgent cases the decision to issue the warrant must then be approved by a Judicial Commissioner before the warrant is issued.

Authorisation of a Part 5 warrant: law enforcement capabilities and delegates

Authorisation by appropriate delegates

5.47 Where it is not reasonably practicable for a law enforcement chief to issue a warrant an appropriate delegate (listed in Schedule 6 of the Act) may exercise the power to issue the warrant instead in an urgent situation. This is distinct to the process outlined for senior officials in paragraph 5.46. In these circumstances the appropriate delegate is not signing a warrant on behalf of the relevant law enforcement chief but is issuing the warrant itself. As such, where an appropriate delegate exercises the power to issue a warrant they must follow the same process that would otherwise be followed by a law enforcement chief. Except in urgent cases, the decision to issue the warrant must then be approved by a Judicial Commissioner before the warrant is issued.

Authorisation of capabilities

5.48 Law enforcement chiefs (and appropriate delegates where applicable) may only issue an equipment interference warrant if they consider that it is necessary and proportionate for the warrant to be issued to their appropriate law enforcement officer. In addition to the factors set out in paragraph 4.18above, in considering whether it is proportionate, they 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 has 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.

5.49 The Secretary of State may issue further guidance to assist law enforcement chiefs and appropriate delegates in considering whether it is proportionate to issue an equipment interference warrant. Taking into account these broader considerations when deciding whether or not to issue a warrant will ensure that equipment interference techniques are deployed by law enforcement agencies in an appropriate, consistent and proportionate manner.

Consideration of collateral intrusion

5.50 Before authorising applications for equipment interference warrants, the person issuing the warrant should consider 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 a relevant legislature (as defined in section 111) and another person on constituency business may be involved. 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.

5.51 A person applying for an equipment interference warrant must also consider appropriate measures to reduce the extent of collateral intrusion. These circumstances and measures will be taken into account by the issuing authority and Judicial Commissioner when considering an application for the issue of an equipment interference warrant.

5.52 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.

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 where there is no longer an authorised purpose for its retention.

5.53 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.

5.54 Should an equipment interference operation reach the point where individuals other than the subject of the authorisation are identified as investigative targets in their own right, for example when interfering with equipment used by more than one person, consideration should be given to applying for separate warrants covering those individuals or, in the case of thematic warrants, modifying the warrant to add those individuals if permissible.

Judicial commissioner approval

5.55 Before a targeted warrant can be issued, the decision to issue it must be approved by a Judicial Commissioner. Section 108 of the Act sets out the test that a Judicial Commissioner must apply when deciding whether to approve the decision. The Judicial Commissioner will review the warrant issuer's conclusions as to whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved. In reviewing those conclusions, the Judicial Commissioner will apply the same principles as would apply on an application for judicial review. The Judicial Commissioner must review the conclusions with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

5.56 The Judicial Commissioner may seek clarification from the warrant granting authority or warrant seeking agency as part of their considerations.

5.57 If the Judicial Commissioner refuses to approve the decision to issue a warrant the issuing authority may either:

- not issue the warrant; or,
- refer the matter to the IPC for a decision (unless the IPC has made the original decision). An urgent warrant which is not approved by a judicial commissioner cannot be appealed to the IPC.

5.58 If the IPC refuses the decision to issue a warrant the issuing authority must not issue the warrant. There is no further avenue of appeal available under the Act.

5.59 Where a Judicial Commissioner refuses the decision to issue the warrant, they must provide written reasons for doing so.

Urgent authorisation of a targeted equipment interference warrant

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

5.61 Urgency is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the time available to meet an operational or investigative need. Accordingly urgent warrants can authorise equipment interference when issued by the issuing authority without prior approval from a Judicial Commissioner. Urgent warrants should fall into one or both of the following 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 or investigative opportunity with limited time to act -- 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.

5.62 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.

5.63 If the Judicial Commissioner approves 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 warrants. Where the issuing authority decides to renew an urgent warrant prior to its approval by a Judicial Commissioner, the original decision to issue the urgent warrant may be considered by the Judicial Commissioner at the same time as they are considering the issuing authority's decision to renew the warrant. A diagram illustrating the process is provided in Annex A.

Duration of equipment interference warrants

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

5.65 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.

5.66 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 those periods.

5.67 Where modifications to an equipment interference warrant are made, the warrant expiry date remains unchanged.

5.68 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 notify the issuing authority. .

Renewal of a targeted equipment interference warrant

5.69 Section 117 of the Act sets out that the appropriate person may renew a warrant. Applications for renewals of warrants should contain an update of the matters outlined in paragraph 5.31 or 5.34 . 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.

5.70 Sections 111 (Members of Parliament etc.), 112 (items subject to legal professional privilege) 113 (confidential journalistic material) and 114 (sources of journalistic material) apply in relation to the renewal of warrants in the same way as they apply to a decision to issue a warrant.

5.71 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.

5.72 In those circumstances where the assistance of a communication service provider or other person has been sought, a copy of the warrant renewal instrument (or part of that instrument that is relevant to the particular communication service provider or other person) 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.

Modification of warrants issued under Part 5

5.73 Warrants issued under Part 5 may be modified under the provisions of section 118 to 124 of the Act. These sections set out the types of modifications that can be made and the process for authorising such modifications.

5.74 An equipment interference warrant may require modification for a number of reasons including a change in circumstances or where new information becomes available that was not known previously. Separate processes apply for the modification of warrants issued by a Secretary of State or Scottish Minister and warrants issued by law enforcement chiefs, these are detailed below. This section should be read in conjunction with the sections in this code on the subject-matter of targeted warrants. 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.

5.75 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. X'. The issuing authority, with Judicial Commissioner approval, issues the warrant authorising the interference of equipment of 'Mr. X'. The investigation progresses and the equipment interference agency wants to interfere with the equipment of one of 'Mr. X's' associates. This would require a new warrant – the warrant against 'Mr. X 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 as part of a single investigation relating to a serious criminal known as 'Mr. X' and his associates 'Mr Y' and 'Mr Z'. The issuing authority, with Judicial Commissioner approval, issues the warrant authorising the interference with equipment used by Mr. X and his associates investigated under Operation "NAME". The investigation progresses and the equipment interference agency wants to interfere with the equipment of another one of Mr. X's associates 'Miss A'. The warrant could be modified to add the equipment used by 'Miss A' subject to the modification provisions of the Act.

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 section 10*1(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 section, 101(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.*

5.76 The requirement to modify a thematic warrant varies depending upon the modification that is being sought and how the matter details are named or described in the warrant. For more information refer to paragraph 5.21.

5.77 In accordance with s118(5) and 123(11), an equipment interference agency is permitted to amend a warrant (including the name or description included in relation to the subject-matter) as long as such an amendment does not alter the conduct that is authorised by that warrant. An example of this would be to correct the spelling of a person's name.

Modification of warrants issued by the Secretary of State or Scottish Ministers

5.78 In the case of a warrants issued by the Secretary of State or Scottish Ministers by virtue of section 102, 103 or 104 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.

5.79 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.

5.80 Section 121 provides that as soon as is reasonably practicable after a person makes a modification to a warrant under section 118, 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 5.84);
- judicial approval would already be required to carry out the modification by virtue of sections 111 to 114; or
- the modification is to remove any matter, name or descriptions included in the warrant.

Modification of warrants issued by a law enforcement chief

5.81 In the case of warrants issued by a law enforcement chief by virtue of section 106, section 123 provides that a modification may be made by the following persons in circumstances where the person considers that the modification is necessary on any relevant grounds:

- A law enforcement chief; or
- if the warrant was issued by an appropriate delegate, by that person.

5.82 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, except where the person who made the modification considered that there was an urgent need to make it, (wherein different modification provisions are provided for, detailed below at paragraph 5.85).

Urgent modification of targeted warrants

5.83 Sections 122 and 124 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 and where the activity required is not authorised by the existing equipment interference warrant.

5.84 For the security and intelligence agencies, a senior official in the equipment interference agency may make an urgent modification to a warrant issued under Part 5, but it must be approved by a senior official in the warrant granting department within three 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 (further detail is provided in paragraph 5.86 onwards). The Secretary of State should be informed of any additional interference that has been authorised.

5.85 In the case of law enforcement agencies, the relevant law enforcement chief or an appropriate delegate may make an urgent modification to a targeted equipment interference warrant. The decision to make the modification must then be approved by a Judicial Commissioner within three working days. In the event that the Judicial Commissioner does not approve the decision, the activity conducted under the urgent modification remains lawful. In such circumstances 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 (further detail is provided in paragraph 5.86 onwards). Where a Judicial Commissioner refuses to approve the urgent modification, there is no route of appeal for the issuing authority to the IPC.

Warrants and modifications ceasing to have effect and authorisation of further interference

5.86 Where a Judicial Commissioner refuses to approve a decision to issue an urgent warrant, or where the Secretary of State, senior official or Judicial Commissioner refuses to approve an urgent modification, the equipment interference agency must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant or modification stops as soon as possible.

5.87 Where any such action cannot be stopped without further interference, the Act permits the person who refused to approve the urgent warrant or modification to authorise further interference for the purpose of enabling the person to whom the warrant was addressed to secure that anything in the process of being done under the warrant, or modification, stops as soon as possible.

5.88 In order to seek authorisation for further interference the equipment interference agency may make representations to the person who refused to approve the urgent warrant or modification.

5.89 When considering whether to authorise further interference the person who refused to approve the urgent warrant or modification should consider whether further interference will result in an overall reduction to the amount of intrusion in to privacy. They should consider how long further interference should be permitted for and exactly what interference is to be permitted.

5.90 If a person determines that further interference is appropriate they should communicate their decision to the equipment interference agency in writing setting out exactly what interference the agency is authorised to undertake, for how long they are able to carry out the interference and under what circumstances the further interference should cease. The written authorisation will make lawful any further interference conducted by the agency in accordance with that authorisation. There are no provisions for extending, modifying or renewing authorisations of further interference. A record of any authorised further interference should be kept by the equipment interference agency.

Example: An equipment interference agency has sought an urgent targeted equipment interference warrant in order to install a piece of software on a suspected terrorist's mobile phone. The issuing authority authorises the urgent warrant, so the agency begins the operation. Two working days later the Judicial Commissioner considers the urgent warrant application and determines that they will not approve the decision to issue the warrant. The activity being carried out must cease as soon as is reasonably practicable, but the equipment interference agency are unable to remove the software without further interference. In the interest of minimising ongoing interference with privacy the Judicial Commissioner may make lawful further interference in accordance with the provisions of the Act code.

5.91 Any further interference authorised in this way must not equate to activity authorised by an equipment interference warrant as defined in section 99 (2) of the Act in that the main purpose of the interference being considered must not be to obtain communications, equipment data or other information. However, if the obtaining of communications, equipment data or other information is required for the purpose of securing that anything in the process of being done under the warrant or modification stops as soon as possible, then the further interference can be authorised as the obtaining of such material is necessary in order to fulfil the intended purpose of the interference. The Judicial Commissioner, Secretary of State or senior official may dictate whether such information is destroyed and may impose conditions on its use. Example 2: The equipment interference agency in 'Example 1' has been authorised to proceed with further interference in order to remove software from a mobile phone. The equipment interference agency explained to the Judicial Commissioner that in order to remove the software they would inevitably receive a small amount of equipment data from the mobile phone. As the purpose of the interference is to remove the software, and not to gather new intelligence, the further interference was correctly authorised without the need for a new equipment interference warrant.

5.92 Where a Judicial Commissioner refuses to approve an urgent warrant they may direct that any of the material obtained under the warrant is destroyed and impose conditions as to the use or retention of any of that material. The equipment interference agency may make representation to the Judicial Commissioner to inform them of any information that they may wish to consider whilst making their determination. Section 110 (5) of the Act requires the Judicial Commissioner to have regard to any such representation.

Warrant cancellation

5.93 Any of the persons authorised to issue warrants under Part 5 may cancel a warrant at any time. In addition, a senior official acting on behalf of the issuing authority may cancel a warrant. If an appropriate person[10] 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.

5.94 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..

5.95 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 everyone on whom the warrant was served since it was issued or last renewed.

Combined warrants

5.96 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.

5.97 Schedule 8 to the Act provides for combined warrants. Combining warrant applications is not mandatory, but provides the option for grouping warrant and authorisation for the same investigation/operation together so that the issuing authority and/or Judicial Commissioner can consider the full range of actions that may be undertaken in relation to the investigation. It allows a more informed decision about the necessity and proportionality of the totality of the action being undertaken and may be more efficient for the agency applying for the warrant as it reduce duplication of identical information across warrant applications.

---

[10] Section 125(4) define ‘appropriate persons’

Example 1: 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 conducted when on the premises 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 could therefore be issued by the relevant person (Secretary of State or law enforcement chief) and approved by a Judicial Commissioner.

Example 2: 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 interception. The interception cannot be authorised as incidental conduct so a combined interception and equipment interference warrant, or separate authorisations must be obtained. A combined warrant may be issued by the Secretary of State and approved by a Judicial Commissioner.

Example 3: An equipment interference agency wishes to conduct an operation which involves directed surveillance in order observe a subject's activity (provided for under Part 2 of RIPA) and targeted equipment interference in order to acquire the subject's communications. 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 issue the combined warrant. This combined warrant would also require approval by a Judicial Commissioner.

5.98 For combinations of warrants under schedule 8, the authorisation process set out at paragraph 5.44onwards 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 one of the warrants or authorisations within a combined warrant is cancelled, the whole warrant ceases to have effect under the same procedures set out at paragraph 5.93. For example, if conduct required for an operation was authorised by a combined equipment interference and interception warrant and interception was no longer necessary and proportionate, the whole warrant must be cancelled and a new equipment interference warrant sought to cover the equipment interference that remains necessary and proportionate. Combined warrants may also be applied for on an urgent basis.

5.99 Where warrants of different durations are combined, the shortest duration applies, except for where a combined warrant issued on the application of the head of an intelligence service and with the approval of a Judicial Commissioner includes an authorisation for directed surveillance – in this case, the duration of the warrant is six months.

5.100 The requirements that must be met before a warrant can be issued apply to each part of a combined warrant. So, for example, where a combined warrant includes a targeted equipment interference warrant, all the requirements that would have to be met for a targeted equipment interference warrant to be issued should be met by the combined warrant.

5.101 The duties imposed by section 2 (having regard to privacy) apply to combined warrants as appropriate. The considerations that apply when deciding whether to issue, renew, cancel or modify a Part 5 warrant will apply when such a warrant forms part of a combined warrant. So the targeted equipment interference element of a combined warrant cannot be issued without having regard to privacy in accordance with section 2.

5.102 In seeking the assistance of a third party to give effect to a warrant it is possible to serve only the relevant part of a combined warrant. For example, if a combined warrant included a targeted equipment interference warrant and an authorisation for directed surveillance, and the target equipment interference required the assistance of a third party, it is possible to serve just the part of the warrant that relates to the targeted equipment interference warrant on that third party.

5.103 Paragraph 20 of Schedule 8 provides that various rules regarding warrants apply separately to the relevant part of a combined warrant. The duty of operators to give effect to a warrant applies separately in relation to each part of a combined warrant. So, for example, section 128 (duty of telecommunications operators to assist with implementation) would apply to the targeted equipment interference part of a combined warrant but only to that part.

5.104 Similarly, safeguards also apply to individual parts of a combined warrant. For instance, where a combined targeted equipment interference and intrusive surveillance warrant has been issued, the safeguards that apply to a targeted equipment interference warrant apply to the part of the combined warrant that is a targeted equipment interference warrant. Section 132 (duty not to make unauthorised disclosures) and 134 (the offence of making unauthorised disclosures) apply to the targeted equipment interference part of a combined warrant.

5.105 The exclusion of matters from legal proceedings (section 56) 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 in principle be used in legal proceedings if required. However, if material derived from equipment interference authorised by a combined warrant reveals the existence of an interception warrant the material is excluded from use in legal proceedings according to section 56 of the Act.

5.106 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

5.107 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 102 with one or more of the following:

- A targeted examination warrant under section 19(2) or section 102(3),
- A directed surveillance authorisation under section 28 of RIPA,
- An intrusive surveillance authorisation under section 32 of RIPA,
- A property interference authorisation under section 5 of the Intelligence Services 1994.

5.108 Paragraph 4 of Schedule 8 sets out that a Scottish Minister may issue a warrant combining a targeted interception warrant under section 21 with a targeted equipment interference warrant and/or a targeted examination warrant under section 103.

5.109 Paragraph 10 of Schedule 8 sets out that a Scottish Minister may issue a warrant combining a targeted equipment interference warrant under 103 (1) with:

- A targeted examination warrant under section 103(2),
- A targeted examination warrant under section 21(2),
- A property interference authorisation under section 5 of the Intelligence Services Act 1994.

5.110 The Secretary of State's decision to issue a combined warrant requires the approval of a Judicial Commissioner in the same way as the decision to issue an equipment interference warrant. The double lock applies to combined warrants. However, where a warrant under section 5 of the Intelligence Services Act forms part of the combined warrant, paragraph 21(3) of Schedule 8 sets out that the Judicial Commissioner does not have the same role in relation to that part of the application.

Example: A security and intelligence agency wishes to conduct an operation which involves property interference (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.

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

5.111 Paragraph 2 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.

5.112 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 equipment interference warrant with one or more of the following:

- A directed surveillance authorisation under section 28 of RIPA,
- An intrusive surveillance authorisation under section 32 of RIPA.

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

5.113 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 28 of RIPA,
- An intrusive surveillance authorisation under section 32 of RIPA,
- A property interference authorisation under the 1997 Act.

5.114 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

5.115 Any person applying for an equipment interference warrant should consider whether there are any relevant 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.

5.116 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.

5.117 Where a person or organisation outside of the public authority is acting under direction of an equipment interference agency, any activities they conduct which comprise equipment interference for the purposes of the Act, should be considered for authorisation under the Act.

5.118 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.

5.119 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 specified within the warrant application, including why the assistance of an international partner is required. 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 99(5) (b) of the Act.

Collaborative working – law enforcement agencies

5.120 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.

5.121 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 who 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.

5.122 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.

5.123 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 3.28).

5.124 In cases where one equipment interference agency is acting on behalf of another, the tasking agency should 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 appropriate for another agency to obtain the warrant that other agency must obtain the equipment interference warrant. For example, where a police force considers that there is not sufficient resource available to ensure the protection of a sensitive technique, it may approach the NCA to obtain the warrant.

5.125 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. This does not prohibit an equipment interference agency working with other persons or organisations where such assistance was not foreseen.

6 Bulk equipment interference warrants

6.1 This chapter applies to the bulk equipment interference by means of a warrant issued under Chapter 3 of Part 6 of the Act. A bulk equipment interference warrant may only be issued to the security and intelligence agencies and must meet two conditions. The first is that its main purpose must be limited to the acquisition of overseas-related communications, equipment data and/or information. Overseas-related communications, equipment data and information are defined at section 176 of the Act. This condition prevents the issue of a bulk equipment interference warrant with the primary purpose of obtaining communications, equipment data or information of people in the British Islands.

6.2 The second condition is that the warrant authorises or requires the person to whom it is addressed to obtain the communications, equipment data or other information described in the warrant and/or to select for examination such material. A bulk equipment interference warrant must set out specified operational purposes (see also paragraph 6.62). No material may be selected for examination unless doing so is necessary for one or more of the operational purposes specified on the warrant.

Bulk equipment interference in practice

6.3 Bulk equipment interference warrants are described in section 176 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.

6.4 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.

6.5 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. The following example demonstrates the difference between thematic and bulk equipment interference:

Example: Intelligence suggests that a terrorist 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, officers 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.

The selection for examination of material obtained under a bulk equipment interference warrant

6.6 Section 178 of the Act requires that a bulk equipment interference warrant must specify the operational purposes for which any material obtained under the warrant may be selected for examination. It is highly likely that a bulk equipment interference warrant will specify the full range of operational purposes (in accordance with section 183(6)); this is explained in more detail in the "Examination Safeguards" section of this chapter.

6.7 In addition, other than in exceptional circumstances, it will always be necessary and proportionate for all the operational purposes included in the central list of operational purposes maintained by the heads of the security and intelligence agencies to be specified in relation to the selection for examination of any material obtained under a bulk equipment interference warrant that is not protected material.

6.8 When an authorised person within the equipment interference agency selects material for examination, documentation must exist that provides an explanation of why it is necessary for one or more of the operational purposes specified on the warrant, and why it is proportionate. This process is subject to internal audit and external oversight by the IPC.

6.9 Where an authorised person wishes to select for examination protected material of a person in the British Islands collected under a bulk equipment interference warrant, additional safeguards will apply and a separate application will need to be made for a targeted examination warrant (see also paragraph 5.34].

Format of warrant application

6.10 An application for a bulk equipment interference warrant is made to the Secretary of State. As set out at section 178 of the Act, bulk equipment interference warrants are only available to the security and intelligence agencies. In this chapter, reference to an 'application' for a warrant includes the application form and the draft warrant (including the draft instrument and any draft schedules). 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.

6.11 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). A bulk warrant must always be necessary in the interests of 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 each of the operational purposes specified.

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

a. Background to the application;

b. A general description of the equipment to be interfered with and the communications, information and equipment data to be obtained;

c. Description of the conduct to be authorised, the main purpose of which must be the obtaining of overseas-related communications, overseas-related information or overseas-related equipment data, as well as any conduct it is expected will be necessary to undertake in order to carry out what is authorised or required by the warrant;

d. 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;

e. 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;

f. Consideration of whether material obtained under the warrant may be made available to any other security and intelligence agency or an international partner, where it is necessary and proportionate to do so;

g. 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;

h. 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 what is sought to be achieved by the warrant could not reasonably be achieved by other less intrusive means;

i. 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 193 of the Act;

j. Where an application is urgent, the supporting justification; and

k. An assurance that all material will be kept for no longer than necessary and handled in accordance with the safeguards required by section 191 of the Act.

Authorisation of a bulk equipment interference warrant

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

Necessity

6.14 Before a bulk equipment interference warrant can be issued, the Secretary of State must consider that the warrant is necessary for one or more of the statutory purposes, as at 178(1)(b) and (2). One of these statutory purposes must always be national security. If the Secretary of State is not satisfied that the warrant is necessary in the interests of national security, then it cannot be issued.

6.15 Before a bulk equipment interference warrant can be issued, 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 178(1)(d)). Setting out the operational purposes on the warrant limits the purposes for which material collected under the warrant can be selected for examination. When considering the specified operational purposes, the Secretary of State must also be satisfied that 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 178(1)(b)). 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, the selection for examination for each specified operational purpose on that warrant must be necessary for one or both of these two broader purposes. In cases where it is necessary and proportionate for material obtained under the warrant to be made available to another of the security and intelligence agencies or an international partner, the operational purposes specified in the warrant may include operational purposes relating to that third party providing the tests in section 178(1)(d) are met.

6.16 The Secretary of State has a duty to ensure that arrangements are in force for securing that only material which has been considered necessary for examination for a section 178(1)(b) or section 178(2) purpose, and which meets the conditions set out in section 193 is, in fact, selected for examination. The IPC is under a duty to review the adequacy of those arrangements.

Proportionality

6.17 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.

6.18 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

6.19 Before deciding to issue a warrant, the Secretary of State must consider that satisfactory arrangements are in force in relation to the warrant, covering the copying, dissemination and retention of material. These safeguards are explained in Chapter 9 of this code.

Authorisation of a bulk equipment interference warrant: senior officials

6.20 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.

Judicial Commissioner Approval

6.21 Before a bulk equipment interference warrant can be issued, the Secretary of State's decision to issue it must be approved by a Judicial Commissioner. Section 140 of the Act sets out the test that a Judicial Commissioner must apply when considering whether to approve the decision. The Judicial Commissioner will review the Secretary of State's conclusion as to whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved. The Judicial Commissioner will also review the Secretary of State's conclusions as to whether each of the operational purposes specified on the warrant is a purpose for which selection is, or may be, necessary.

6.22 In reviewing these conclusions, the Judicial Commissioner will apply the same principles as would apply on an application for judicial review. The Judicial Commissioner must review the conclusions with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

6.23 The Judicial Commissioner may seek clarification from the warrant granting department or warrant seeking agency as part of their considerations.

6.24 If the Judicial Commissioner refuses to approve the decision to issue a warrant the Secretary of State may either:

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

6.25 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 in the Act.

6.26 Where a Judicial Commissioner refuses the decision to issue the warrant, they must provide written reasons for doing so.

Urgent authorisation of bulk equipment interference warrants

6.27 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 time available to meet an operational or investigative need. Accordingly, urgent warrants can authorise equipment interference when issued by the issuing authority without prior approval from a Judicial Commissioner. Urgent warrants should fall into at least one of the following three categories:

- Imminent threat to life or serious harm - for example, if a terrorist attack is imminent which could be prevented or mitigated using bulk equipment interference;
- An intelligence gathering or investigative opportunity with limited time to act - for example, a terrorist group are known to be operating from a certain region, but are likely to relocate imminently.

6.28 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.

6.29 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.

6.30 The diagram in Annex B illustrates the bulk equipment interference urgent authorisation process.

Warrants and modifications ceasing to have effect and authorisation of further interference

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

6.32 Where this is not possible, the Act permits the Judicial Commissioner to authorise further interference for the purpose of enabling the person to whom the warrant was addressed to secure that anything in the process of being done under the warrant, or modification, stops as soon as possible.

6.33 In order to seek authorisation for further interference the equipment interference agency may make representations to the Judicial Commissioner who refused to approve the urgent warrant or modification.

6.34 When considering whether to authorise further interference the Judicial Commissioner should consider whether further interference will result in an overall reduction to the amount of intrusion in to privacy. They should consider how long further interference should be permitted for and exactly what interference is to be permitted.

6.35 If the Judicial Commissioner determines that further interference is appropriate they should communicate their decision to the equipment interference agency in writing setting out exactly what interference the agency is authorised to undertake, for how long they are able to carry out the interference and under what circumstances the further interference should cease. The written authorisation will make lawful any further interference conducted by the equipment interference agency in accordance with that authorisation. There are no provisions for extending, modifying or renewing authorisations of further interference. A record of any authorised further interference should be kept by the equipment interference agency in accordance with paragraph10.9of this code.

6.36 Any further interference authorised in this way must not equate to activity authorised by a bulk equipment interference warrant as defined in section 176 (1) of the Actin that the main purpose of the interference being considered must not be to obtain overseas-related communications, equipment data or other information. However, if the obtaining of such communications, equipment data or other information is required for the purpose of securing anything in the process of being done under the warrant or modification stops as soon as possible, the further interference can be authorised as the obtaining of such material is necessary in order to fulfil the intended purpose of the interference.. The Judicial Commissioner may dictate whether such information is destroyed and may impose conditions on its use.

6.37 Where a Judicial Commissioner refuses to approve an urgent warrant they may direct that any of the material obtained under the warrant is destroyed and impose conditions as to the use or retention of any of that material. The equipment interference agency may make representation to the Judicial Commissioner to inform them of any information that they may wish to consider whilst making their determination. Section 181 (4) of the Act requires the Judicial Commissioner to have regard to any such representation.

Format of a bulk equipment interference warrant

6.38 A bulk equipment interference warrant will comprise a warrant instrument signed by the Secretary of State (and may also include a schedule or set of schedules). 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 will include the following:

- A statement that it is a bulk equipment interference warrant;
- The person to whom it is addressed, which will be the head of the security and intelligence agency by whom, or on whose behalf, the application was made;
- 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;
- Date the warrant was issued; and
- The warrant reference number.

Duration of bulk equipment interference warrants

6.39 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.

6.40 Where modifications to a bulk equipment interference warrant are made, the warrant expiry date remains unchanged.

Renewal of a bulk equipment interference warrant

6.41 The Secretary of State may renew a bulk equipment interference warrant within the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect (section 185 of the Act) with the approval of the Judicial Commissioner. Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 6.12 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 178(2), and why it is considered that the conduct authorised by the warrant continues to be proportionate.

6.42 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 (at 178(1)(b) and 178(2)).

6.43 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.

6.44 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 have effect from 2 January.

6.45 In those circumstances where the assistance of a communication service provider or other person has been sought, a copy of the warrant renewal instrument (or part of that instrument that is relevant to the particular communication service provider or other person) 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.

Modification of a bulk equipment interference warrant

6.46 A bulk equipment interference warrant may be modified by an instrument under the provisions at section 186 of the Act. The modifications that can be made to a bulk equipment interference warrant are:

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

6.47 In the case of **major modifications**, 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 6.14 - 6.18 apply to a modification as they do to the issuing of a new warrant.

6.48 The major 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 warrant a new warrant should be sought. The Act permits that when it is not reasonably practicable for the Secretary of State to sign a major modification instrument a delegate may sign it on their behalf. Typically this scenario will arise where the 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 modification. In circumstances where a modification is being made to add or vary an operational purpose, once the modification has come into force, the added or varied operational purpose may be used to select for examination any material obtained under the warrant, even if this material was obtained prior to the addition or variation of the operational purpose.

6.49 In the case of **minor modifications**, the modification may be made by the Secretary of State or by a senior official acting on their behalf. If a minor modification, 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 must modify the warrant to remove that operational purpose.

6.50 A bulk equipment interference warrant authorises the acquisition of material, and 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 acquisition of material. 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 of material already obtained under the warrant.

6.51 Such a modification is a **minor modification** and may be made by the Secretary of State or by a senior official acting on their behalf. In circumstances where such a modification is being made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

6.52 In accordance with s118(5) an equipment interference agency is permitted to amend a warrant (including the names or descriptions included in relation to the subject-matter) as long as such an amendment does not alter the conduct that is authorised by that warrant. An example of this would be to correct incorrect spelling.

Urgent modification of a bulk equipment interference warrant

6.53 In urgent cases a major modification can be made by a Secretary of State. An urgent case may be where a sudden terrorist incident requires the urgent selection for examination of the data already held for an operational purpose not listed on the warrant or where a very limited window of opportunity to act requires a modification to the conduct authorised by the warrant.

6.54 Where a major modification is made in an urgent case, a statement of that fact must be included on the modifying instrument, and the modification must be approved within three working days following the date of issue by a Judicial Commissioner. 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. In such cases section 186 of the Act requires the warrant to contain a statement confirming that it was not reasonably practicable for the instrument to be signed by the Secretary of State, and that the Secretary of State has personally and expressly authorised the making of the modification If a Judicial Commissioner refuses to approve the modification, the modification will cease to have effect. That refusal does not affect the lawfulness of anything done between the modification being made and the Judicial Commissioner reviewing and refusing the modification.

6.55 The Judicial Commissioner may approve further interference (see paragraph 6.41), but only in the interest of ensuring that anything being done by virtue of the modification is stopped as soon as possible.

6.56 Where a Judicial Commissioner refuses to approve the urgent modification, the Secretary of State may not refer the case to the Investigatory Powers Commissioner.

Warrant cancellation

6.57 Section 189 of the Act provides that the Secretary of State, or a senior official acting on their behalf, may cancel a bulk equipment interference warrant at any time. Such a person 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.

6.58 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.

6.59 The Act requires the person to whom a warrant is addressed 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.

6.60 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 other persons, if any, who have given effect to the warrant.

Examination safeguards

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

6.61 Section 193 of the Act provides specific safeguards relating to the selection for examination of material acquired through a bulk equipment interference warrant. Further guidance on these safeguards is provided below.

6.62 Sections 193(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, in line with section 183 of the Act. Operational purposes limit the purposes for which data collected under the warrant can be selected for examination. 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.

6.63 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 be required over time. Section 183 of the Act makes clear that the heads of the security and intelligence agencies must maintain a central list of all of the operational purposes, separate to individual bulk warrants, which they consider are purposes for which material may be selected for examination. The maintenance of this list will ensure the agencies are able to assess and review all of the operational purposes that are, or could be, specified across the full range of their bulk warrants at a particular time to ensure these purposes remain up to date, relevant to the current threat picture and, where applicable, the intelligence priorities set by the National Security Council. The central list of operational purposes will not be limited to operational purposes relevant to bulk equipment interference warrants. This list must provide a record of all of the operational purposes that are specified, or could be specified, on any bulk interception, bulk acquisition, bulk equipment interference or bulk personal dataset warrant and, as far as possible, the operational purposes specified on the list should be consistent across these capabilities. Some operational purposes on the central list 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.

6.64 Section 183 also makes clear that an operational purpose may not be specified on an individual bulk warrant unless it is a purpose that is specified on the central list maintained by the heads of the security and intelligence agencies. And before an operational purpose may be added to that list, it must be approved by the Secretary of State. In practice, the addition of one operational purpose to the list will often require the approval of more than one Secretary of State. For example, where an operational purpose is being added to the list that is likely to be specified on bulk warrants issued to each of the three security and intelligence agencies, that operational purpose will need to be approved by both the Home Secretary and Foreign Secretary.

6.65 Section 178 makes clear that the operational purposes specified on a bulk warrant must relate to one or more of the statutory purposes specified on that warrant. However, section 183 makes clear that it is not sufficient for any operational purpose simply to use the wording of one of the statutory purposes. The Secretary of State may not approve the addition of an operational purpose to the central list – and therefore to any bulk warrants – unless he or she is satisfied that the operational purpose is specified in a greater level of detail than the relevant statutory purposes. Operational purposes must therefore describe a clear requirement and contain sufficient detail to satisfy the Secretary of State that material may only be selected for examination for specific reasons.

6.66 Section 186 of 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. Such a modification is categorised as a major modification and must be made by the Secretary of State and approved by a Judicial Commissioner before the modification may take effect. In such circumstances, and as outlined above, the provisions at section 183 also require that the operational purpose must be approved by the Secretary of State for addition to the central list. If the Secretary of State does not approve the addition of the purpose to the list, the modification to the warrant (to add a new operational purpose) may not be made. The Act therefore creates a strict approval process in circumstances where an intelligence agency identifies a new operational purpose, which they consider needs to be added to a bulk warrant. The Secretary of State must agree that the operational purpose is a purpose for which selection for examination may take place, and that it is described in sufficient detail such that it should be added to the central list. In addition, the Secretary of State must also consider that the addition of that purpose to the relevant bulk warrant is necessary, taking into account the particular circumstances of the case, before making the modification, and the decision to add the operational purpose must also be approved by a Judicial Commissioner.

6.67 In addition to the central list of operational purposes having to be approved by the Secretary of State, section 183 makes clear that it must also be reviewed on an annual basis by the Prime Minister and it must be shared every three months with the Intelligence and Security Committee of Parliament.

6.68 Although bulk equipment interference warrants are authorised for the purpose of acquiring overseas-related communications, overseas-related equipment data, or overseas-related information, section 176(5) of the Act includes bulk equipment interference warrants authorising the acquisition of such material that are not overseas-related to the extent this is necessary in order to acquire the overseas-related communications to which the warrant relates. Operational purposes specified on the central list maintained by the heads of the security and intelligence agencies –and on individual bulk equipment interference warrants – may therefore include purposes that enable the selection for examination of protected material or other data of individuals in the UK. The safeguards in section 193 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 protected material (see also Chapter 5)[11].

6.69 The analysis of bulk systems data and identifying data is the primary means by which the security and intelligence agencies are able to discover and assess threats to the UK. This can only be achieved effectively through the aggregation of systems data and identifying data from a wide range of sources acquired under multiple bulk warrants. Such analysis allows the agencies to draw together fragments of information into coherent patterns, which allow for the identification of those threats while at the same time minimising intrusion into privacy.

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

6.71 No data may be selected for examination other than in accordance with the specified operational purposes. In general, automated systems should, where technically possible, be used to effect the selection for examination in accordance with section 193 of the Act. A limited number of officials may also be permitted to access the system during the processes of filtering, processing and selection for examination, for example to check system health. Such access must itself be necessary on the grounds specified in sections 178(1)(b) and (2) and where such access involves selection for examination of content or secondary data it must be necessary for an operational purpose specified on the warrant. Agency arrangements for such access will be kept under review by the IPC during his or her inspections.

[11] Where there is a change of circumstances such that a person whose communications' content is being selected for examination enters, or is discovered to be in the British Islands, sections 193(5) and (6) provide for a continuity arrangement.

6.72 Material 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 193 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 security cleared.

6.73 No material may be selected for examination for the specified operational purposes unless this is necessary and proportionate in all the circumstances. In addition, arrangements must be put in place to provide for the creation and retention of documentation (for the purposes of subsequent examination or audit) outlining why access to the material by authorised persons is necessary and proportionate and the applicable operational purposes. Systems should, to the extent possible, prevent access to the material unless such documentation has been created. The documentation must also record the reasons why any collateral intrusion into privacy is considered proportionate and any steps to minimise it. All documentation must be retained in accordance with agreed policy for the purposes of subsequent examination or audit.

6.74 Authorised persons may be granted access to systems containing material obtained under a bulk equipment interference warrant only for defined periods of time, after appropriate training, and where it is necessary for them to have access. Access may be renewed where these conditions continue to be met.

6.75 Periodic audits should be carried out to ensure that the requirements set out in section 193 of the Act are being met. These audits must include checks to ensure that the documentation justifying selection for examination have been correctly compiled, and specifically, that the material 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.

6.76 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.

6.77 The Prime Minister must approve any application to select for examination the communications or private information of a member of a relevant legislature obtained under a bulk equipment interference warrant.

6.78 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.

6.79 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 any material obtained under a bulk equipment interference warrant that is not protected material.

Selection for examination of protected material in breach of the section 193(4) prohibition

6.80 Any selection for examination of protected material must also meet the selection conditions set out at section 193(3) and (4). Section 193(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 that individual's protected material. 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 193(5).

6.81 Selection in breach of the prohibition in section 193(4) of the Act may be authorised by section 193(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 to the British Islands. To enable the selection for examination to continue, sections 193(5) and 193(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 193(5), the Secretary of State must be notified.

Offence of breaching examination safeguards

6.82 Material obtained under a bulk equipment interference warrant may only be selected for examination subject to the safeguards in sections 193 and 194 of the Act. Section 196 of the Act makes it an offence for a person to deliberately select such material for examination in breach of these safeguards where that person knows or believes such selection does not comply with the safeguards.

7 Implementation of warrants and Communication Service Provider compliance

7.1 After a warrant has been issued, it will be forwarded to the person to whom it is addressed – i.e. the equipment interference agency which submitted the application.

7.2 Section 128 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.

7.3 Section 127 makes clear that the warrant may be served on any person, inside or outside the UK, who may be able to provide such assistance in relation to that warrant. The same process applies for bulk equipment interference warrants and is set out at section 149 of the Act.

7.4 Where a copy of an equipment interference warrant has been served on anyone offering or providing a telecommunications service to a person in the UK, or who has control of, or provides a telecommunications system which is wholly or partly in the UK, that person is under a duty to take all such steps for giving effect to the warrant as are notified to the person by or on behalf of the equipment interference agency. This applies to any company offering or providing services to persons in the UK, irrespective of where the company is based. Section 128 sets out the means by which that duty may be enforced.

7.5 Section 128 of the Act[12] 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 (section 149 of the Act makes clear that sections 42 and 43 apply in relation to a bulk equipment interference warrant as they do for a targeted equipment interference warrant):

- 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, or any other means, are reasonably practicable). The equipment interference agency must take steps to bring the contents of the warrant to the attention of the relevant person.

Provision of reasonable assistance to give effect to a warrant

7.6 Any communication service provider, 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 capable of providing 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 127).

7.7 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 128(5)).

[12] By virtue of section 191 of the Act, section 128 (service of warrants) applies in relation to bulk equipment interference warrants as it applies in relation to targeted warrants.

7.8 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 128(2)). Section 128(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. Only law enforcement officers from specified law enforcement agencies are able to apply for equipment interference warrant that include a duty on providers to assist with implementation, namely – the NCA, HM Revenue and Customs, the Police Services of Scotland and Northern Ireland and the Metropolitan Police Service.

7.9 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 communication service provider, or details about the technical specification of relevant equipment.

7.10 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 communication service provider employees required to assist with implementation; and
- What measures should be taken to minimise any impact upon the communication service provider and their employees so far as is practicable.

7.11 In some cases equipment interference agencies may consider that the same material can be acquired either with assistance of a communication service provider 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 4.18.

7.12 The steps which may be required by communication service providers are limited to those which it is reasonably practicable to take (section 128(5)). What is reasonably practicable will be considered on a case-by-case basis, taking into account the individual circumstances of the relevant communication service provider, and any consultation between the communication service provider and the equipment interference agency. Such consultation is likely to include discussion of a number of factors including, but not limited to, the technical feasibility and likely cost of complying with any steps notified to the communication service provider. As part of the consultation the communication service provider 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.

7.13 A copy pf the warrant must be served in such a way as to bring the contents of the warrant to the attention of the person or communications service provider who the equipment interference agency considers can provide assistance in relation to it. The agency may provide the following to the person or communication service provider:

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

7.14 An optional covering document from the equipment interference agency (or the person acting on behalf of the agency) may also be provided to notify the communications service provider of steps they are required to take to give effect to the warrant 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 communication service providers who maintain a technical capability. The communications service provider should be provided with enough information to enable them to carry out the interference in relation to their system(s) but will not necessarily be provided with all the information contained in the warrant.

7.15 Sections 99(5)(b) and 176(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 communication service providers 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 sections 99(5)(b) or 176(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 99(5)(b) or 176(5)(b)..

7.16 Section 237 provides that disclosures can be made to the Investigatory Powers Commissioner. This includes disclosures made by communications service providers who can contact the Commissioner at any time to request advice and guidance.

Duty not to disclose the existence of a warrant

7.17 For guidance on the provision for communications service providers to be able to publish information in relation to the number of warrants they have given effect to, see paragraph 9.3.

Contribution of costs for giving effect to an equipment interference warrant

7.18 Section 249 of the Act recognises that communication service providers incur costs in complying with requirements in the Act, including equipment interference in response to requests under Part 5 of the Act. The Act, therefore, requires the Secretary of State to have in place arrangements to ensure that operators receive an appropriate contribution to these costs.

7.19 Public funding and support is made available to communication service providers 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 to protect the public and to bring to justice those who commit serious crime or are involved in acts of terrorism. The provision of public funding may be subject to terms and conditions determined by the Secretary of State.

7.20 It is legitimate for a communication service provider to seek contributions towards its costs which may include an element of funding towards those general business overheads required in order to facilitate the timely implementation of an equipment interference warrant. This is especially relevant for communication service providers which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke systems. However, certain staff benefits or arrangements made in line with the terms and conditions of employment, such as bonuses paid to members of staff that are reflective or representative of the company's performance, will be excluded from this category of costs.. Such matters are arranged between the employer and employee and the Government does not accept responsibility for such costs. Further details with respect to cost recovery will be available in the handbook provided to all communication service providers who maintain an equipment interference capability.

7.21 Contributions may also be appropriate towards costs incurred by a communication service provider 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 for the interference.

7.22 Any communication service provider seeking to recover appropriate contributions towards its costs should make available to the Secretary of State such information as the Secretary of State requires in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the communication service provider.

7.23 Any communication service provider that has claimed contributions towards costs may be required to undergo any audit that may be reasonably required 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.

8 Maintenance of a technical capability

8.1 Communications service providers may be required under section 253 of the Act to provide a technical capability notice to give effect to interception, equipment interference and bulk acquisition warrants and notices or authorisations for the acquisition of communications data. The purpose of maintaining a technical capability is to ensure that, when a warrant, authorisation or notice 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 interception or equipment interference capability, although they may be obligated to give effect to a warrant.

8.2 The Secretary of State may give a relevant communication service provider 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. The Secretary of State may only give a notice where the decision to do so has been approved by a Judicial Commissioner. In practice, technical capability notices will only be given to communication service providers that are likely to be required to give effect to warrants, authorisations or notices given under Part 3 of the Act on a recurrent basis.

8.3 The only obligations that may be imposed by a technical capability notice are those set out in regulations made by the Secretary of State and approved by Parliament. Section 253(4) limits the obligations that the Secretary of State may include in those regulations. =

8.4 Section 253(5) gives examples of the sorts of obligations that such regulations may include:

- 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.

8.5 An obligation can only be imposed by a technical capability notice for the purpose of securing that it is (and remains) practicable to impose requirements on a communication service provider, and that the provider is capable of providing the necessary technical assistance to meet these requirements. For example, an obligation relating to the security of a telecommunications service or system can be imposed by a technical capability notice for the purpose of ensuring that the operator has the capability to provide assistance in relation to an equipment interference warrant.

8.6 An obligation imposed by a technical capability notice on a communications service provider to remove encryption does not require the provider to remove encryption per se. Rather, it requires that provider to maintain the capability to remove encryption when subsequently served with a warrant, notice or authorisation. Such an obligation may only relate to electronic protections that the company has itself applied to material or where those protections have been applied on behalf of that communication service provider and not to encryption applied by any other party. References to protections applied on behalf of the communication service provider include circumstances where the communication service provider has contracted a third party to apply electronic protections to a telecommunications service provided by that communication service provider to their customers.

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

8.8 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, an equipment interference warrant may require a communications service provider to take such steps as are reasonably practicable to take to give effect to it. This will include, where applicable, providing material in an intelligible form. An example of such circumstances might be where a communication service provider removes encryption from material for their own business reasons.

Consultation with service providers.

8.9 Before giving a notice, the Secretary of State or delegated official must consult the communication service provider[13]. In practice, informal consultation is likely to take place long before a notice is given. The Government will engage at the outset with communication service providers 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.

[13] See section 255(2).

8.10 In the event that the giving of a notice to a communication service provider is deemed necessary and proportionate, the Secretary of State must consult the communication service provider formally before the notice is given. Again, the Secretary of State may delegate participation in this exercise to officials. Should the communication service provider have concerns about the reasonableness, cost or technical feasibility of the obligations to be set out in the notice, these should be raised during the consultation process. At the conclusion of these discussions, any outstanding concerns must be taken into account by the Secretary of State as part of the decision making process.

Matters to be considered by the Secretary of State

8.11 Following the conclusion of consultation with a communication service provider, the Secretary of State will decide whether to give a notice. This consideration should include all the aspects of the proposed notice and its effect on the communications service provider. 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.

8.12 As part of the decision the Secretary of State must take into account, amongst other factors, the matters specified in section 255(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 necessity of the capability but also the likely benefits;
- The technical feasibility of complying with the notice – taking into account any representations made by the communication service provider and giving specific consideration to any obligations in the notice to remove electronic protections (as described at section 255(4));
- The likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the communication service provider 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 communication service provider – again taking into account any representations made by the company.

8.13 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 (2) of the Act also requires the Secretary of State to give regard to the following when giving, varying or revoking a notice so far as they are relevant:

- 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.

8.14 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 limited to those set out in regulations made by the Secretary of State under section 253, as described above

8.15 Before the notice may be given, a Judicial Commissioner must approve the Secretary of State's decision to give the 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 as to whether the notice is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved. In reviewing these conclusions, the Judicial Commissioner will apply the same principles as would apply on an application for judicial review. In addition, the Judicial Commissioner must review the conclusions with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

Giving a notice

8.16 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 communication service provider. 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.

8.17 Section 255(6) 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 communication service provider[14]:

- 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

[14] See section 255(6).

- At an address in the UK specified by the person.

8.18 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.

8.19 As set out in section 253(7), the notice will specify the period within which the communication service provider 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.

8.20 The notice will also specify the telecommunications services or systems to which the obligations will apply.

8.21 A person to whom a technical capability notice is given is under a duty to comply with the notice.

Disclosure of technical capability notices

8.22 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 that have been given a notice. Should criminals become aware of the capabilities of the equipment interference agencies, they may alter their behaviours and change communication service provider, making it more difficult to detect their activities of concern.

8.23 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[15].

8.24 Section 255(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 might include disclosure:

- To a person (such as a system provider) who is working with the communication service provider to give effect to the notice;
- To relevant oversight bodies;
- To a legal advisor in contemplation of legal proceedings, or for the purpose of those proceedings;

[15] See section 255(8).

- To regulators, in exceptional circumstances where information relating to a capability may be relevant to their enquiries;
- To other communication service providers 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.

Regular review

8.25 Section 256(2) of the Act imposes an obligation on the Secretary of State to keep technical capability notices under regular review. This helps to ensure that the notice itself, or any of the requirements specified in the notice, remain necessary and proportionate. This evaluation differs from the review process provided for in section 257 of the Act, which permits communications service providers to request a review of the requirements placed on them in a technical capability notice should they consider these to be unreasonable.

8.26 It is recognised that, after a notice is given, the communication service provider 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.

8.27 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.

8.28 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 communication service provider's activities or services; or
- a significant refresh or update of communication service provider's systems.

8.29 When reviewing a technical capability notice, the Secretary of State must consult the communications service provider in deciding whether the notice remains necessary and proportionate.

8.30 A review may conclude that the notice should continue to remain in force, be varied to add or remove obligations, or be revoked. The relevant communication service provider and the equipment interference agencies will be notified of the outcome of the review.

Variation of technical capability notices

8.31 The communications market is constantly evolving and communication service providers subject to technical capability notices will often launch new services.

8.32 Communications service providers which have been given a technical capability notice must notify the Secretary of State of changes to existing telecommunications services and the development of new services and relevant products in advance of their launch. This will enable the Secretary of State to consider whether it is necessary and proportionate to require the communications service provider company to modify an existing capability or provide a new technical capability on the service.

8.33 Certain changes to services, such as upgrades of systems which are already covered by the existing notice, may be agreed between the Secretary of State and communications service provider in question where the change would not require new obligations to be imposed on the company. However, significant changes to networks or service which necessitate new obligations being imposed on the company will require a variation of the technical capability notice.

8.34 Section 256 of the Act provides that technical capability notices may be varied by the Secretary of State if the Secretary of State considers that the variation is necessary and the conduct required by the variation is proportionate to what is sought to be achieved. Where the variation imposes new obligations on the communications service provider, the decision to vary a notice must be approved by a Judicial Commissioner. Judicial Commissioner approval is not required where a variation removes obligations from the notice.

8.35 There are a number of reasons why a notice might be varied. These include:

- a communication service provider launching new services;
- changing equipment interference agency demands and priorities;
- a recommendation following a review (see paragraph 8.30 above); or
- to amend or enhance the security requirements.

8.36 Where a communication service provider 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 communication service provider, will need to consider whether the existing notice should be varied.

8.37 Before varying a notice, the Secretary of State is required to consult the communications service provider to understand the impact of the change, including cost and technical implications. The Secretary of State, or officials to whom the exercise has been delegated should also consult the equipment interference agencies to understand the operational impact of any change to the notice.

8.38 Further detail on the consultation process and matters to be considered by the Secretary of State can be found above at paragraph 8.9 above.

8.39 Once a variation has been agreed by the Secretary of State, and the decision to vary a notice has been approved by a Judicial Commissioner, arrangements will be made for the communication service provider to receive notification of this variation and details of the timeframe in which the variation needs to be enacted by the communication service provider. 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

8.40 A technical capability notice must be revoked (in whole or in part) if it is no longer necessary to require a communication service provider to provide a technical capability or if it is no longer reasonable to impose certain obligations on the provider.

8.41 Circumstances where it may be necessary to revoke a notice include where a communication service provider 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.

8.42 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 communication service provider in the future should it be considered necessary and proportionate to do so.

Referral of technical capability notices

8.43 A person to whom a notice is given may request a review of any aspect of a technical capability notice should they wish to do so. A person may refer the whole or any part of the notice back to the Secretary of State for review under section 257 of the Act.

8.44 The circumstances and timeframe within which a communication service provider 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 communication service provider 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.

8.45 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.

8.46 The Commissioner and the TAB must give the relevant communication service provider 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.

8.47 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 IPC must approve the decision. Until the Secretary of State's decision is approved, there is no requirement for the communication service provider to comply with the notice so far as referred. Notwithstanding the review, the communication service provider may be required to provide assistance in giving effect to a warrant or authorisation.

Contribution of costs for the maintenance of a technical capability

8.48 Section 249 of the Act recognises that communication service providers incur expenses in complying with requirements in the Act, including notices to maintain technical capabilities under Part 9. The Act, therefore, requires the Secretary of State to have in place arrangements to ensure that communication service providers receive an appropriate contribution to these costs.

8.49 Communication service providers 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.

8.50 Any contribution towards these costs must be agreed by the Secretary of State before work is commenced to develop, install, or operate the capability. Furthermore, the Secretary of State must be satisfied that the proposed capability will meet the requirements set out in the notice.

8.51 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 communication service providers in complying with their obligations outlined above. This is particularly relevant for communication service providers that employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems. However, certain staff benefits or arrangements made in line with the terms and conditions of employment, such as bonuses paid to members of staff that are reflective or representative of the company's performance, will be excluded from this category of costs. Such matters are arranged between the employer and employee and the Government does not accept responsibility for such costs. Further details with respect to cost recovery will be available in the handbook provided to all communications service providers who maintain an equipment interference capability. .

8.52 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 communication service provider expands or changes its network for commercial reasons, it is expected to meet any capital costs that arise.

General considerations on appropriate contributions

8.53 Any communication service provider seeking to recover appropriate contributions towards its costs should make available to the Government such information as the Secretary of State requires in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the communication service provider.

8.54 As costs are reimbursed from public funds, communication service providers 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, communication service providers should take this into account when altering business systems and must notify the Secretary of State of proposed changes.

8.55 Any communication service provider that has claimed contributions towards costs may be required to undergo any audit that may be reasonably required before contributions are made by the Secretary of State. 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

8.56 In certain circumstances it may be more economical for apparatus, systems or other facilities or services required to enable or facilitate communication service providers to comply with obligations under the Act to be developed centrally, rather than communication service providers 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).

8.57 Section 250 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 communication service providers to acquire material. Such systems could operate in respect of multiple powers under the Act.

8.58 Where such systems are developed for use by communication service providers, the Secretary of State will work closely with communication service providers to ensure the systems can be properly integrated into their networks. Communication service providers 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

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

8.60 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

8.61 Each communications service provider to whom a notice is given 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.

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

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

Personnel Security

8.64 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.

8.65 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.

8.66 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 cleared. On an annual basis, managers must identify any concerns that may lead to the security clearance of individual members of staff being reconsidered. The security clearance of each individual member of staff must also be periodically reviewed.

8.67 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

8.68 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.

8.69 Equipment used to for the purpose of warranted equipment interference must be sanitised and securely disposed of at the end of its life[16].

Operations management

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

8.71 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.

8.72 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.

8.73 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

8.74 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.

---

[16] Please see 8.77for further details on the disposal of equipment interference systems.

8.75 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.

8.76 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

8.77 The requirement that when destroying data it must be deleted in such a way that it 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.

8.78 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.

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

8.80 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 under this Act or another enactment.

9 Safeguards (including privileged or confidential information)

9.1 All material obtained under the authority of an equipment interference warrant must be handled in accordance with safeguards which the issuing authority has approved in line with the duty imposed on him or her by the Act. These safeguards are made available to the IPC, and they must meet the requirements of section 129 for Part 5 warrants and section 191 for Part 6 warrants. Breaches of these safeguards must be reported to the IPC in a fashion agreed with him or her. 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.

9.2 Sections 129 and 191 of the Act require that disclosure, copying and retention of material is limited to the minimum necessary for the authorised purposes. Sections 129(3) and 191(3) of the Act provide that something is necessary for the authorised purposes if the material:

- Is, or is likely to become, necessary for any of the purposes set out in section 129(7) for targeted warrants or 178 (2) for bulk warrants – namely, 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 relevant to national security or in the interest of the prevention of death or injury;
- 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.

9.3 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.

Duty not to make unauthorised disclosure and excepted disclosures

9.4 Section 132 imposes a duty on those individuals listed in subsection (3) not to disclose the existence or contents of a warrant, details of the issue of the warrant or any renewal or modification of the warrant, the existence or content of any requirement to provide assistance in giving effect to a warrant, steps taken in pursuance of the warrant or any material obtained under a warrant. Section 134 sets out the offence for an individual who makes an unauthorised disclosure.

9.5 Section 133 of the Act sets out the meaning of "excepted disclosure" and the circumstances in which disclosure made in relation to a warrant is permitted. Section 133 is broken down into a number of types of circumstances (or "heads) in which disclosure would be an "excepted disclosure".

9.6 **Head 1** includes where it is authorised by the warrant, authorised by the person to whom the warrant is addressed or authorised by terms of any requirement to provide assistance in giving effect to the warrant.

9.7 **Head 2** provides for disclosures to or authorised by a Judicial Commissioner and disclosure to the Independent Police Complaints Commission or the Intelligence and Security Committee of Parliament for the purpose of carrying out its functions.

9.8 **Head 3** provides for disclosure by a legal adviser in contemplation of or in connection with any legal proceedings, or disclosure by a professional legal advisor to his or her client, or vice versa, for the purpose of giving advice about relevant provisions of the Act.

9.9 **Head 4** provides for disclosure of statistics by telecommunications operators in accordance with regulations made by the Secretary of State. The regulations may allow the publication of statistics relating to the number of warrants to which they have given effect Head 4 also includes when a disclosure is made, not only in relation to a particular warrant but in relation to equipment interference warrants in general.

9.10 Disclosure may also be subject to other duties of confidentiality, for example, from contractual agreements. In particular, the exceptions in section 133 do not override duties imposed by the Official Secrets Act 1989 or other requirements of vetting. In practice, this means that any disclosure to or by lawyers under this section will require reasonable measures to be taken to ensure that sensitive material is properly protected.

Disclosures authorised by the warrant or the person to whom the warrant is addressed

9.11 Head 1 (see section 133(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 any requirements imposed by virtue of 129 of the Act and chapter 9 of this Code.

9.12 The issuing authority, or the person to whom a warrant is addressed, may consider it is appropriate to authorise a disclosure where, for example, a communication service provider requests the ability to disclose the existence of a warrant to a relevant regulator for audit or regulatory purposes. In this case the issuing authority or the person to whom the warrant is addressed may consider that such a disclosure would be in the public interest, would not risk the viability of any equipment interference techniques and that the requirements of 126(4) would be met.

Offence of making unauthorised disclosure

9.13 Section 134 of the Act makes it 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 132(3). The offence does not apply however if:

- The disclosure is an excepted disclosure according to section 133. 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.

Use of material as evidence

9.14 Subject to the provisions in this chapter of the 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[17] and the Human Rights Act 1998.

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

9.15 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 under the authority of an equipment interference warrant is used evidentially, the equipment interference agency should be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

9.16 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. For law enforcement equipment interference agencies, consideration should be had to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996.

9.17 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.

Reviewing warrants

9.18 Regular reviews of all warrants should be undertaken during their life time to assess the necessity and proportionality of the conduct. Particular attention should be given to the need to review warrants frequently where the interference involves a high level of intrusion into private life or significant collateral intrusion, or particularly sensitive information is likely to be obtained. As set out at section 2(2)(b) of the Act, at the point the equipment interference authority is considering applying for a warrant, they must have regard to whether the level of protection to be applied in relation to information obtained under the warrant is higher because of the particular sensitivity of that information.

9.19 In each case, unless specified by the issuing authority, 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.

9.20 In the event that there are any significant and substantive changes to the nature of the interference during the currency of the warrant, the equipment interference agency should consider whether it is necessary to apply for a new warrant.

Dissemination of material obtained under an equipment interference warrant

9.21 Material acquired through equipment interference will need to be disseminated both within and between agencies, as well as to consumers of intelligence (which includes oversight bodies and the Secretary of State for example), where necessary in order for action to be taken on it. 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 set out in section 129(3) and 191(3) of the Act. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside an agency. It is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle: material acquired by virtue of equipment interference must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the material to carry out those duties. In the same way, only so much of the material may be disclosed as the recipient needs. For example, if a summary of the material will suffice, no more than that should be disclosed.

9.22 The obligations apply not just to the original equipment interference authority, 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 original agency's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients.

9.23 Sections 130 and 192 of the Act stipulate that where material obtained under an equipment interference warrant is disclosed to the authorities of a country or territory outside the UK, the appropriate issuing authority must ensure that the material is only handed over to the authorities if the following requirements are met:

- It appears to the issuing authority that the requirements corresponding to the requirements in section 129(2) and (5) for Part 5 warrants, or 191(2) and (5) for bulk warrants (relating to minimising the extent to which material is disclosed, copied, distributed and retained) will apply to the extent (if any) that the issuing authority considers appropriate;

- Where unselected data obtained under a bulk warrant is disclosed to overseas authorities, it appears to the Secretary of State that requirements corresponding to the requirements of section 193 (safeguards relating to the examination of material) will also apply to the extent (if any) that the Secretary of State considers appropriate;

Copying

9.24 Material may only be copied to the extent necessary for the authorised purposes set out in sections 129(3) and 191(3) of the Act. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify the material as having been obtained under a warrant , and any record referring to the interference and which is a record of the identities of the persons to whom the material relates.

Storage

9.25 All copies, extracts and summaries of material acquired by equipment interference must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store material securely applies to all those who are responsible for handling it, including those assisting with the implementation of a warrant. The details of what such a requirement will mean in practice for any communications service providers that are required to provide assistance will be set out in the discussions they have with the Government before being asked to give effect to a warrant (see chapter 7 of this code).

9.26 In particular, each equipment interference agency must apply the following protective security measures:

- Physical security to protect any premises where the information may be stored or accessed;
- IT security to minimise the risk of unauthorised access to IT systems;
- a security clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Destruction

9.27 Material acquired under an equipment interference warrant, and all copies, extracts and summaries of material which can be identified as the product of an equipment interference warrant, must be scheduled for deletion and securely destroyed as soon as possible, once it is no longer needed for any of the authorised purposes. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible[18]. If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 129(3) or, in the case of a bulk warrant, section 191(3) of the Act.

[18] For example, by taking reasonable steps to make the data unavailable or inaccessible to authorised persons. No further steps are required, such as physical destruction or hardware.

9.28 Where a security and intelligence agency undertakes interference under a bulk warrant, the agency must specify (or must determine on a system by system basis) maximum retention periods for different categories of the data which reflect its nature and intrusiveness. The specified periods should normally be no longer than two years, and should be agreed with the IPC. Where material is stored on a system, they will not be stored for the purpose of IPC oversight beyond the retention period already set for that system. Data may only be retained for longer than the applicable maximum retention periods if prior authorisation is obtained from a senior official within the particular agency on the basis that continued retention of the data has been assessed to be necessary and proportionate. If continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, it must be deleted. So far as possible, all retention periods should be implemented by a process of automated deletion, which is triggered once the applicable maximum retention period has been reached for the data at issue.

9.29 Any collateral material that has been acquired over the course of a testing or training exercise should be destroyed as soon as reasonably possible when the purpose of the testing or training exercise has been fulfilled. For example, it may take a period of time to go through the data to check whether the equipment has worked properly. It may also be appropriate in some cases to retain test data and re-run this rather than cause further intrusion by carrying out further interference.

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

9.30 Where material is obtained by an 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 had it been obtained directly by the authority under the authority of an equipment interference warrant.

Confidential or privileged information

9.31 Particular consideration should be given to the acquisition of material or the selection for examination of material where individuals might reasonably assume a high degree of confidentiality. This includes where the material contains information that is legally privileged (see paragraphs 9.39 to 9.63); confidential journalistic material or where material identifies a journalist's source (see paragraphs 9.64to 9.78); where material contain confidential personal information or material is that of a member of a relevant legislature.

9.32 Section 111 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 Prime Minister must also be consulted before a decision is made to renew a warrant and prior to making a modification of a warrant in respect of a member of a relevant legislature. In a case where section 111 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.

Confidential personal information and communications between a member of a relevant legislature and another person on constituency business

9.33 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. Authorised persons in the equipment interference agencies should receive appropriate training on the safeguards regarding confidential or privileged information

9.34 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.

9.35 Where the intention is to acquire confidential personal information, or communications between a member of a relevant legislature (as defined in section 2) and another person on constituency business the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the information is exchanged with the intention of furthering a criminal purpose, for example, if purported spiritual counselling involves incitement to murder or to acts of terrorism, then the information will not be considered confidential for the purposes of the Act. If the acquisition of confidential personal or constituency business 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.

9.36 Where confidential personal or constituency business information is retained and disseminated to an outside body, reasonable steps should be taken to mark the disseminated 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.

9.37 Any case where confidential personal or constituency business information is retained, other than for the purposes of destruction, and dissemination should be notified to the IPC as soon as reasonably practicable.

9.38 The safeguards set out above also apply to any material obtained under a bulk equipment interference warrant which is selected for examination and which constitutes confidential or constituency business information and is retained other than for the purpose of its destruction.

Items subject to legal privilege

9.39 Section 98 of the Police and Criminal Evidence Act 1984 describes those matters that are subject to legal privilege in England and Wales. In Scotland, those matters subject to legal privilege are defined in Section 263 of the Investigatory Powers Act. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.

9.40 Legal privilege does not apply to material held with the intention of furthering a criminal purpose (whether the legal adviser is acting unwittingly or culpably). Privilege is not lost where a professional legal adviser is 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 a member of the legal profession, such as advocates, barristers, solicitors or chartered legal executives.

9.41 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 considered in accordance with section 112 of the Act 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.

9.42 Sections 112 and 194 of the Act provide 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. Section 112 provides for three different circumstances where legally privileged items will or may be obtained or selected for examination. They are; i) where privileged material is likely to be obtained or selected for examination; ii) where privileged material is intentionally sought, or selected for examination; and iii) where the purpose or one of the purposes is to obtain items subject to legal privilege that, if they were not made or held with the intention of furthering a criminal purpose, would be subject to privilege. Further guidance is set out below as to what should be done in each of those cases.

Application process for targeted warrants that are likely to result in acquisition of items subject to legal privilege

9.43 Section 112 of the Act sets out the processes that must be followed where a targeted equipment interference warrant may obtain or select for examination items subject to legal privilege. Different processes apply depending on whether obtaining or examining items subject to legal privilege is the purpose (or one of the purposes) of the warrant, or whether it is not the purpose but is nevertheless likely. Subsections (8) and (9) set out the process where the purpose of the warrant is not to obtain or examine items subject to legal privilege, but where the equipment interference agency considers it likely that the warrant would authorise or require the acquisition of items subject to legal privilege, or in the case of an examination warrant, where the warrant would authorise the selection for examination of material that is likely to include items subject to legal privilege. In such cases the warrant application must be clear that the warrant would authorise the acquisition of material likely to include items subject to legal privilege and must include an assessment of how likely it is that items which are subject to legal privilege will be obtained. This is in addition to the application setting out the reasons why it is considered necessary for acquisition or examination to take place. In the application, the relevant agency should confirm that any items that are subject to legal privilege that are inadvertently obtained 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.

Application process for warrants where the purpose, or one of the purposes, is to obtain or examine items subject to legal privilege

9.44 Where the intention is to acquire items subject to legal privilege, the warrant application must contain a statement that the purpose, or one of the purposes, of the warrant is to obtain legally privileged material. Section 112 provides that the warrant may only be issued if the issuing authority is satisfied that there are exceptional and compelling circumstances that make the warrant necessary, and the Judicial Commissioner approves that decision. Section 112 also sets out that circumstances cannot be exceptional and compelling unless certain conditions are met. Exceptional and compelling circumstances will arise only in a very restricted range of cases. Section 112 states that a warrant to target such material can only be issued where there is a risk of death or significant injury or in the interests of national security. The exceptional and compelling test can only be met when the public interest in obtaining the information sought outweighs the public interest in maintaining the confidentiality of legally privileged material, and when there are no other reasonable means of obtaining the required information. The interference must be reasonably regarded as likely to yield the intelligence necessary to counter the threat.

Example: An equipment interference 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.

9.45 Further, in considering any such application, the issuing authority and Judicial Commissioner must be satisfied that the proposed conduct is proportionate to what is sought to be achieved and must have regard to the public interest in the confidentiality of items subject to privilege. They will wish to consider carefully whether the activity or threat being investigated is of a sufficiently serious nature to override the public interest in preserving the confidentiality of privileged communications, and the likelihood that the information sought will have a positive impact on the investigation. The issuing authority will take into account both the public interest in preserving the confidentiality of those particular items and the broader public interest in maintaining the confidentiality of items subject to legal privilege more generally. The issuing authority must consider that there are exceptional and compelling circumstances that make it necessary to issue the warrant and must be satisfied that there are appropriate arrangements in place for the handling, retention, use and destruction of privileged items, and the Judicial Commissioner must approve the issuing authority's decision. In such circumstances, the issuing authority will be able to impose additional requirements such as regular reporting arrangements, so as to keep the warrant under review more effectively.

9.46 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.

Application process for warrants where the requesting agency considers that the items are likely to be created or held to further a criminal purpose

9.47 Where an application for a warrant is made where the purpose or one of the purposes is to obtain items that, if they were not created or held with the intention of furthering a criminal purpose, would be subject to privilege and where the requesting agency considers that the items are likely to be created or held to further a criminal purpose, the application must include a statement to that effect and the reasons for believing that the items are likely to be created or held to further a criminal purpose. For example, if the requesting agency had reliable intelligence that a criminal fugitive was seeking advice from a lawyer in order to obtain a false alibi or to assist them in evading arrest, then this may provide grounds for an assessment that the communications with the lawyer will not be privileged, notwithstanding the fugitive appeared to be seeking advice from a lawyer in a professional capacity, and this information should be set out in the application. The requirement to ensure the case for a warrant is presented in the application in a fair and balanced way, including information which supports or weakens the case for the warrant which applies to warrant applications (as set out in paragraph 5.32) applies in these circumstances as it does elsewhere. For example, information which may undermine the assessment that material is likely to be created or held to further a criminal purpose must also be included in the application to ensure the issuing authority can make an informed assessment about the nature of the material. The warrant can only be issued where the issuing authority considers that the targeted items are likely to be created or held with the intention of furthering a criminal purpose.

9.48 In a case where section 112 (items subject to legal privilege) applies in relation to making a modification to a warrant, the same safeguards will apply as apply when a warrant is issued.

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

9.49 In line with section 194 of the Act, where the material obtained under a bulk equipment interference warrant is to be selected for examination according to criteria that are intended to, or are likely to result in, identifying items subject to legal privilege, the enhanced procedure described at paragraph 9.49 and 1applies. This only applies where the individual is outside the British islands, otherwise the relevant targeted examination warrant application would address these considerations as described in paragraphs 9.43 to 9.48.

9.50 An authorised person in a public authority must notify a senior official[19] before criteria to select any protected material for examination, where this will, or is likely to, result in the identification of legally privileged items. The notification must address the same considerations as described in paragraph 9.43. The senior official, who must not be a member of the equipment interference agency to whom the bulk equipment interference warrant is addressed, must in any case where the intention is to identify items subject to legal privilege, apply the same tests and considerations as described in paragraph 9.43 to 9.48and X (including where there are exceptional and compelling circumstances). The authorised person is prohibited from accessing the items until he or she has received approval from the senior official authorising the selection for examination of the items subject to legal privilege.

9.51 In the event that privileged items are inadvertently and unexpectedly selected for examination (and where the enhanced procedure in paragraph 9.49to 9.51has consequently not been followed), any item so obtained must be handled strictly in accordance with the requirements of section 194 and the provisions of this chapter set out at paragraphs 9.49 to 9.51. No further privileged items may be selected for examination by reference to those criteria unless approved by the senior official as set out in paragraph 9.50

Lawyers' material

9.52 Where a lawyer, acting in this professional capacity, is the subject of a targeted equipment interference warrant or a targeted examination warrant or where his or her material is to be selected for examination in accordance with section 193, it is possible that a substantial proportion of the material which will be obtained or selected for examination will be subject to legal privilege. Therefore, in any case where the subject of a targeted equipment interference warrant or a targeted examination warrant, or the subject of examination, is known to be a lawyer acting in that professional capacity the equipment interference agency must assume that section 112 applies. Equipment interference agencies should provide internal guidance to their staff in relation to determining whether a target is a lawyer acting in this professional capacity.

[19] Senior official is defined in section 135 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.

9.53 The equipment interference agency will wish to consider which of the three circumstances which apply when items subject to legal privilege will or may be obtained (or selected for examination) is relevant, and what processes should therefore be followed. In other words, they will need to consider whether items subject to legal privilege are likely to be obtained or selected for examination; whether items subject to legal privilege are intentionally sought, or selected for examination; or whether the purpose or one of the purposes is to obtain material that, if it was not created or held with the intention of furthering a criminal purpose, would be subject to privilege. This paragraph does not prevent an application being made on the grounds that the lawyer is under investigation for serious criminal offences, in which case, the application or notification must be made on the basis that it is likely to acquire items subject to legal privilege and the additional considerations set out at paragraph 9.43 will apply.

9.54 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

9.55 In addition to safeguards governing the handling and retention of material as provided for in sections 129 and 191 of the Act, authorised persons who analyse material obtained by equipment interference should be alert to any communications or items which may be subject to legal privilege. Sections 131 and 194 of the Act sets out the additional arrangements that apply to legally privileged items where the intention is to retain them for a purpose other than their destruction.

9.56 A legal advisor in the equipment interference agency must be consulted when it is believed that material which attracts privilege is to be retained other than for the purpose of destruction.. The legal advisor is responsible for determining that material is privileged rather than an officer who is involved in an investigation. In cases where there is doubt as to whether material is privileged or not, the Investigatory Powers Commission may be informed who will be able to give a view. 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 129(3). If not, the material should not be retained, other than for the purpose of its destruction.

9.57 Material which has been identified as legally privileged (and is being retained for purposes other than its destruction) should be clearly marked as subject to legal privilege and the IPC must be notified of the retention of the items as soon as reasonably practicable. Paragraph 9.58provides more detail on reporting privileged items to the Commissioner. 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 129(3). Privileged items must be securely destroyed when their 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, for purposes other than their destruction, remains necessary and proportionate for the authorised statutory purposes.

Reporting to the Commissioner

9.58 In those cases where legally privileged items have been acquired or, in the case of items acquired in bulk, selected for examination and retained, the matter should be reported to the IPC as soon as reasonably practicable.

9.59 Section 131 provides that the Commissioner must order the destruction of the item or impose conditions on its use or retention unless the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury. Even if retention is necessary and the public interest in its retention outweighs the public interest in the confidentiality of items subject to legal privilege, the Commissioner may still impose conditions as he considers necessary to protect the public interest in the confidentiality of items subject to privilege. It may be the case in some circumstances that privileged items can be retained when its retention does not outweigh the public interest in the confidentiality of items subject to privilege. This includes, for example, where it is not possible to separate privileged items from those that are not privileged and of intelligence value and where the retention is necessary and proportionate for one of more of the authorised purposes set out in section 129(3). In these circumstances, the Commissioner must impose conditions on the use or retention of the items.

9.60 The IPC will make an assessment of whether the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and of whether retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury. If both of those conditions are met, then the Commissioner may impose conditions as to the use or retention of the items, but the Commissioner is not obliged to do so. If those conditions are not met, the Commissioner must direct that the item is destroyed, or must impose one or more conditions as to the use or retention of the items. The Commissioner must have regard to any representations made by the equipment interference agency about the proposed retention of privileged items or conditions that may be imposed.

Dissemination

9.61 In the course of an investigation, an equipment interference agency will not act on or further disseminate legally privileged items unless it has first informed the IPC that the items have been obtained or selected for examination, except in urgent circumstances. Where there is an urgent need to take action and it is not reasonably practicable to inform the IPC that the material has been obtained, or selected for examination before taking action, the agency may take action before informing the IPC. In such cases, the agency should, wherever possible consult a legal adviser. An equipment interference agency must not disseminate privileged items if doing so would be contrary to a condition imposed by the IPC in relation to those items.

9.62 The dissemination of legally privileged material to an outside body should be accompanied by a clear warning that it is subject to legal privilege, where doing so would not breach the duty not to disclose the existence or contents of a warrant in section 132 (see paragraph 9.13). 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 equipment interference agency, 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.

9.63 In order to safeguard against any risk of prejudice or accusation of abuse of process, equipment interference agencies 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 equipment interference agency 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.

Applications to acquire material relating to confidential journalistic material and journalists sources

9.64 There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously.

9.65 Section 264 of the Act defines confidential journalistic material as:

- In the case of material contained in a communication, journalistic material which the sender of the communication ;
- Holds in confidence, or
- Intends the recipient, or intended recipient, of the communication to hold in confidence;
- In any other case, journalistic material which a person holds in confidence

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

9.67 Section 264(7) sets out when a person holds material in confidence. This is if a person holds material subject to an express or implied undertaking to hold it in confidence or the person holds the material subject to a restriction on disclosure or an obligation of secrecy contained in an enactment. Confidentiality can continue to attach to confidential journalistic material when it is sent to or held by a person who is neither the journalist nor the source (for example, a news editor who has been sent some notes by a journalist).

9.68 Section 113 sets out the safeguards which apply when an equipment interference agency applies for a warrant under Part 5 where the purpose, or one of the purposes, of the warrant is to authorise the acquisition or the selection for examination of material that the agency believes will be confidential journalistic material. The warrant application must contain a statement that the purpose is to authorise or require the acquisition of (or select for examination) material which the equipment interference agency believes will contain confidential journalistic material. The person to whom the application is made may issue the warrant only if they consider that appropriate safeguards relating to the handling, retention use and disclosure of the material are in place. Equipment data alone may not be sufficient to identify a source - consequential action and other information is likely to be required. For example, identifying communications addresses does not in itself provide sufficient information to determine the nature of a relationship.

9.69 A source of journalistic information is an individual who provides material intending the recipient to use it for the purpose of journalism or knowing that it is likely to be so used. Throughout this code any reference to sources should be understood to include any person acting as an intermediary between a journalist and a source.

9.70 Section 114 sets out the safeguards which apply when an equipment interference authority applies for a warrant under Part 5 where the purpose, or one of the purposes is to identify or confirm a source of journalistic information. The application must contain a statement confirming that this is the purpose (or one of the purposes) for the application. The person to whom the application is made may issue the warrant only if they consider that appropriate safeguards relating to the handling, retention, use and disclosure of the material are in place.

9.71 An assessment of whether someone is a journalist (for the purposes of the Act) should be made on all the facts and circumstances available at the time. Consideration should be given, in particular, to the frequency of the individual's relevant activities, the level of personal rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest.

9.72 The acquisition and examination of material under parts 5 and 6 of the Act will be a justifiable interference with an individual's human rights under Articles 8 (right to respect for private and family life) and, in certain circumstances, 10 (freedom of expression) of the European Convention on Human Rights only if the conduct being authorised is necessary, proportionate and in accordance with law.

9.73 Where material is created or acquired with the intention of further a criminal purpose, section 264(5) states that the material is not to be regarded as having been created or acquired for the purpose of journalism. For example if a terrorist organisation is creating videos for the promotion or glorification of terrorism according to the UK legal standard, the material cannot be regarded as journalistic material for the purposes of the Act and will not attract the safeguards set out in sections 113, 114 and 195. Once material has been broadcast, no confidentiality can attach to the material so it is not confidential journalistic material. The fact that a person uses social media tools to communicate does not, in itself, indicate that that person is a journalist or that he or she is likely to be holding confidential journalistic material as defined in the Act.

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

Selection for examination of material obtained under a bulk equipment interference warrant, where the purpose or one of the purposes is to identify a journalist's source or to obtain confidential journalistic material

9.75 Where an authorised person in an equipment interference agency intends to select for examination material obtained under a bulk equipment interference warrant in order to identify or confirm a source of journalistic information (and other than where paragraph 9.70 applies), he or she must notify a senior official[20] before selecting that material for examination. The senior official, who must not be a member of the equipment interference agency to whom the bulk equipment interference warrant is addressed, may only approve the proposed selection for examination if he or she considers that the agency has arrangements in place for the handling, retention, use and destruction of material that identify sources of journalistic information. The authorised person is prohibited from selecting the material for examination until he or she has received approval from the senior official authorising the selection of content identifying or confirming a source of journalistic information.

9.76 Equipment data alone may not be sufficient to identify a source – consequential action and other information is likely to be required. Identifying, for example, communications addresses does not in itself provide sufficient information to determine the nature of a relationship. However, where selection is carried out with the intention that the information obtained will be used as part of the assessment of the identity of a source, this will require senior official authorisation in line with the process at paragraph 9.75.

9.77 Where an authorised person in an equipment interference agency intends to select protected material for examination which the agency believes is confidential journalistic material (and other than where paragraph 9.70 applies), the authorised person in the equipment interference agency must notify a senior official[21] before selecting any protected material for examination. The senior official, who must not be a member of the equipment interference agency to whom the bulk equipment interference warrant is addressed, may only approve the proposed selection for examination if he or she considers that the agency has arrangements in place for the handling, retention, use and destruction of that confidential journalistic material. The authorised person is prohibited from selecting the material for examination until he or she has received approval from the senior official.

[20] Senior official is defined in section 198

[21] Senior official is defined in section 198

Reporting to the Commissioner

9.78 In those cases where confidential journalistic material, or material that identifies a source of journalistic information, have been obtained - or, in the case of bulk equipment interference, where confidential journalistic material, or material that identifies a source of journalistic information, have been selected for examination and retained other than for the purposes of destruction the matter should be reported to the Investigatory Powers Commissioner as soon as reasonably practicable .

10 Record keeping and error reporting

Records

10.1 Records must be available for inspection by the IPC and retained to allow the Investigatory Powers Tribunal 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 targeted equipment interference warrants and bulk equipment interference warrants, and applications made for the renewal of such warrants or modifications to those warrants;
- All warrant Instruments, associated schedules, renewal instruments and copies of modification instruments (if any);
- Where any application is refused, the grounds for refusal as given by the issuing authority or Judicial Commissioner;
- where any application is refused, the grounds for refusal as given by the issuing authority or Judicial Commissioner;
- the result of periodic reviews of the warrants;
- any directions to destroy material and/or conditions as to use or retention of material issued by the Judicial Commissioner on refusal to approve an urgent warrant.

10.2 Records should also be kept of the arrangements for securing that only material which has been determined as necessary is, in fact, read, looked at or listened to. Records should also be kept of the arrangements by which the requirements of sections 129(2) and 191(2) (minimisation of copying and distribution of material) and sections 129(5) and 191(5) (destruction of material) are to be met.

10.3 The issuing authority must keep records of the warrant authorisation process. 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;
- A record of whether, following a refusal of any application by a Judicial Commissioner, there is an appeal to the Investigatory Powers Commissioner.
- Where there is such an appeal and the Investigatory Powers Commissioner also refuses the issuing of an application, the grounds for refusal given.

10.4 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.

10.5 In the case of warrants issued under Part 5 of the Act each equipment interference agency 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 to approve the decision to issue a targeted equipment interference warrant;
- The number of decisions to issue a targeted warrant that were refused by the Investigatory Powers Commissioner, following a referral from the Secretary of State.
- 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 issued by the issuing authority and issued by a senior official or appropriate delegate;
- The number of targeted equipment interference warrants issued 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 warrants issued by the issuing authority in an urgent case;
- The number of targeted warrants issued by the issuing authority in an urgent case where a Judicial Commissioner subsequently refused to approve the decision to issue the warrant;

- The number of renewals to targeted warrants that were made.
- The number of targeted warrants that the issuing authority or 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.

10.6 In the case of a targeted equipment interference warrant that was issued without the approval of a Judicial Commissioner, or a modification that was issued without the approval of the Secretary of State, senior official or Judicial Commissioner, a record of any further interference authorised by that person should be kept should they fail to approve the warrant or modification.

10.7 In the case of warrants issued under Chapter 3 of Part 6 of the Act each equipment interference agency must keep a record of:

- 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 decisions to issue a bulk equipment interference warrant that a Judicial Commissioner refused to 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 approve the decision to issue a bulk equipment interference warrant;
- the number of decisions to issue a bulk equipment interference warrant that were refused by the Investigatory Powers Commissioner, following a referral from the Secretary of State;
- 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 the Secretary of State or Judicial Commissioner refused to approve the renewal of;
- 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.

10.8 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 179(1)(b) purpose(s) specified on the warrant;
- the operational purposes 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 refused to approve; and
- 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 approve the decision modify a bulk equipment interference warrant.

10.9 In the case of a bulk equipment interference warrant that was issued without the approval of a Judicial Commissioner, or a modification that was issued without the approval of the Judicial Commissioner, a record of any further interference authorised by that person should be kept should they fail to approve the warrant or modification.

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

Errors

10.11 This section provides information regarding errors. Proper application of the Investigatory Powers Act 2016 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 a public authority, communications service provider or other persons assisting in giving effect to a warrant.

10.12 Wherever possible, technical systems should incorporate functionality to minimise errors. A person holding a senior position within each equipment interference agency must undertake a regular review of errors.

10.13 An error can only occur in certain circumstances. Where interference is authorised under a targeted or bulk equipment interference warrant, an error can only occur after the interference has commenced. Where selection for examination is authorised under a targeted examination warrant, an error can only occur after that selection has commenced.

10.14 An error must be reported if it is a "relevant error". Section 231 (9) of the Act requires this code to give a description of those errors that also meet the requirements of section 231(9)(a)[22] for an error to be relevant.

10.15 A relevant error occurs in one or more of the following circumstances:

- Equipment interference without lawful authority has occurred[23].
- There has been a failure to adhere to the additional safeguards set out at sections 111 to 114 of the Act.
- There has been a failure to adhere to the restrictions on disclosure of material imposed by sections 129 to 131 and sections 191 to 195 of the Act.

10.16 The following provides a non-exhaustive list of possible relevant errors that would amount to an error by the public authority in complying with the requirements imposed on it[24] and that would fall within the descriptions provided at para 10.15:

- Human error which leads to material from the wrong device being obtained.
- Warranted equipment interference has taken place but the material obtained does not in the event relate to the intended equipment where information held by the equipment interference agency at the time of seeking a warrant could reasonably have indicated this.
- Failure to take all reasonably practicable steps to secure that anything in the process of being done under the warrant stops as soon as possible after the warrant is cancelled.
- A breach of the relevant safeguard section caused by software or hardware errors.
- Selection for examination of material acquired under a bulk equipment interference warrant without a valid operational purpose.
- Retention of data when it is no longer necessary for the authorised purposes.

[22] S231(9)(a) states that it must be an error " by a public authority 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.

[23] For the purposes of this section, equipment interference without lawful authority is when interference with equipment occurs for the purpose of obtaining communications, equipment data or other information without a warrant or other lawful authorisation in place, when one would be required (either under the Act or other legislation). For the avoidance of doubt, this does not include cases in which both (a) no further action is being taken in respect of the means of interference and (b) communications, equipment data or other information are not being sought.

[24] In accordance with section 231(9)(a).

- Selection for examination of material by criteria referable to an individual known to be in the British Islands that is not authorised by a targeted examination warrant or written authorisation under s193(5).

- An equipment interference agency selects for examination an item subject to legal privilege, using criteria designed to identify material subject to legal privilege, without complying with the requirements of section 194.

- An equipment interference agency fails to inform the IPC that it has obtained, or has selected for examination, an item which is legally privileged or which contains confidential journalistic material, and intends to retain it for purposes other than its destruction.

- An equipment interference agency discloses material from a bulk equipment interference warrant to an overseas authority other than in accordance with section 192(1).

10.17 Errors can have very significant consequences on an affected individual's rights and, in accordance with section 235(6) of the Act, all relevant errors must be reported to the Investigatory Powers Commissioner by the public authority or communications service provider that is aware of the error.

10.18 When a relevant error has occurred, the public authority that made the error must notify the IPC ten working days after it has been established by appropriate internal governance processes that a relevant 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.

10.19 From the point at which the public authority identifies that a relevant error may have occurred, they must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the equipment interference agency must also inform the Commissioner of when it was initially identified that an error may have taken place.

10.20 Section 235(6) of the Act also places a requirement on communications service providers to report to the Investigatory Powers Commissioner any relevant error, committed by a public authority, of which they become aware. In such circumstances, the process for reporting the error to the Commissioner at paragraphs 10.18 and 10.19above applies to communications service providers as it applies to public authorities. In addition, the communications service provider should inform the relevant public authority as soon as they become aware that authority may have made an error. The communications service provider may then work in conjunction with the public authority to confirm the fact of the error and report it to the Commissioner.

10.21 A full report must be sent to the Investigatory Powers Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it has not been possible to provide the full report within ten working days of establishing the fact of the error, the reasons this is the case. Where the report is being made by the public authority that made the error that report should also include: the cause of the error; the amount of material 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.

10.22 As set out at section 231(9) of the Act, the Commissioner will keep under review the definition of relevant errors. The Commissioner may also issue guidance as necessary, including guidance on the format of error reports.

10.23 An error that falls within the descriptions provided at paragraph 10.15 but is committed either by a communications service provider or any other person providing assistance with giving effect to a warrant is not a relevant error. However, in addition to the requirement in the Act to report relevant errors to the Commissioner, a public authority or communications service provider should also report to the Commissioner any other error of which they become aware that meets the criteria at paragraph 10.15 of this section. The reporting of such errors will help to draw attention to those aspects of the process that require improvement to eliminate further errors and the undue interference with any individual's rights.

10.24 If a public authority discovers a communications service provider error (which cannot therefore be a relevant error) they should notify the Investigatory Powers Commissioner and the communications service provider of the error straight away to enable the communications service provider to investigate the cause of the error and report it themselves. For example, if an equipment interference agency have instructed a communication service provider to cease interference and have cancelled their warrant but the communication service provider has not terminated the activity.

10.25 In addition to errors, as described in this section, situations may arise where a warrant under Part 5 of the Act has been obtained or modified as a result of the relevant agency having been provided with details of equipment 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 relied in good faith. Whilst these actions do not constitute a relevant error on the part of the agency which acted on the information, such occurrences should be brought to the attention of the Commissioner.

Serious errors

10.26 Section 231 of the Act states that the Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. 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.

10.27 In deciding whether it is in the public interest for the person concerned to be informed of the error, 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 intelligence services.

10.28 Before making his or her decision, the Commissioner must ask the equipment interference agency which has made the error to make submissions on the matters concerned.

10.29 When informing a person of a serious error, the Commissioner must inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

11 Oversight

11.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ('the Commissioner), whose remit includes providing comprehensive oversight of the use of the powers contained within the Act and adherence to the practices and processes described by this code. The Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts and legal experts, qualified to assist the Commissioner in his or her work (the 'Technical Advisory Panel').

11.2 The Commissioner, 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 Commissioner's statutory functions, entirely on his or her own initiative or they may be asked to investigate a specific issue by the Prime Minister. Section 236 also provides for the Intelligence and Security Committee of Parliament to refer a matter to the Commissioner with a view to carrying out an investigation, inspection or audit.

11.3 The Commissioner 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 Commissioner 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, offer all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner.

11.4 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 10 of this code, 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 Investigatory Powers Tribunal (IPT).

11.5 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 10 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.

11.6 The Commissioner must also inform the affected individual of their right to apply to the Investigatory Powers Tribunal (see chapter 12 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.

11.7 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 telecommunications operators 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.

11.8 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: […]

12 Complaints

12.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints regarding 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 against the intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

12.2 The IPT is entirely independent from Her Majesty's Government and the 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.

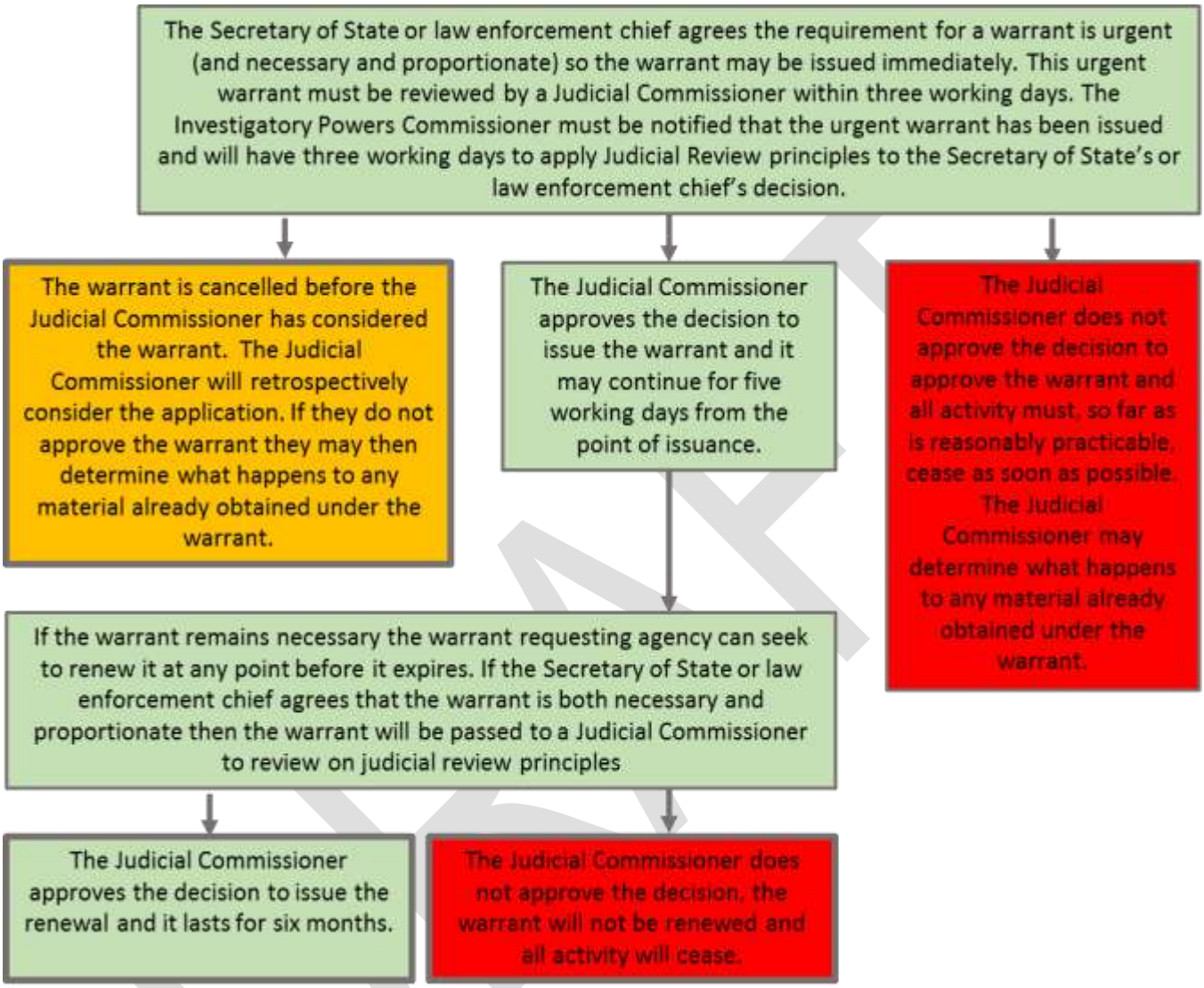
12.3 This code does not cover the exercise of the Tribunal's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: www.ipt-uk.com. Alternatively information on how to make a complaint can be obtained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

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

12.4 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.

13 Annex A

Urgent authorisation of a targeted equipment interference warrant



14 Annex B

Urgent authorisation of a bulk equipment interference warrant