These notes refer to the Regulation of Investigatory Powers Act 2000 (c.23) which received Royal Assent on 28 July 2000

REGULATION OF INVESTIGATORY POWERS ACT 2000

EXPLANATORY NOTES

COMMENTARY ON SECTIONS

For "provide assistance", see subsection (9).

105. *Subsection (2).* Where an intercepting agency requires another person to assist it in implementing an interception, it is likely that the person providing assistance will wish to be satisfied that there is an interception warrant in existence. This subsection provides for this, allowing the intercepting agency to provide either a copy of the warrant or to make arrangements whereby a copy is provided.

106. *Subsection (3).* Where a copy of a warrant is served upon a person providing assistance in accordance with subsection (2), this subsection allows the intercepting agency to restrict the disclosure of the warrant to just that material which the person providing assistance needs to see in order to satisfy themselves that their actions are authorised. Most commonly this may involve a communications service provider only being shown the front of the warrant (showing the name of the person to be intercepted) and the specific schedule which identifies the communications which they are being asked to provide assistance in intercepting.

107. *Subsection (4)* states that where a person providing a communications service is required to give assistance in accordance with an interception warrant, they must do everything required of them by the person to whom the warrant is addressed in order to give effect to the warrant. As to what the warrant authorises or requires, see Section 5.

108. *Subsection (5)* ensures that no unreasonable demands are made of service providers.

109. *Subsection (6)* explains that that where a service provider has had an obligation to provide an intercept capability imposed upon them under Section 12, it is reasonable to expect them to be able to provide assistance with an intercept up to the level of the imposed capability.

110. *Subsection (7)* creates a criminal offence of knowingly failing to comply with a requirement to provide the required assistance in implementing an interception warrant. It goes on to specify the maximum penalties which a person who is found guilty of this offence may be sentenced to. On the statutory maximum, see the note for Section 1(7).

111. *Subsection (8)* also allows the Secretary of State to take civil proceedings against a person who fails to provide the required assistance under subsection (4) in order to compel him to provide such assistance by means of, inter alia, an injunction or other appropriate relief.

112. *Subsection (9)* explains that the term "provision of assistance" includes the actual disclosure of the intercepted material and related communications data to the person to whom the warrant is addressed (or his representative).

Section 12: Maintenance of interception capability

113. This section provides a power allowing the Secretary of State to impose obligations upon providers of publicly available communication services to maintain a reasonable intercept capability.

114. *Subsection (1)* provides the mechanism by which the Secretary of State may set out a framework for obligations upon persons providing or planning to provide public postal services or public telecommunications services. The Secretary of State will do this through an order (affirmative resolution, see subsection (10)) which lays out the obligations which he believes are reasonable, with the aim of ensuring that providers are capable of giving assistance in the implementation of interception warrants. The order itself will not impose specific requirements on providers but will describe in general terms the kind of intercept capability which they may be required to provide.

For the meaning of "public postal service" and "public telecommunications service", see Section 2(1). But see also Section 12(4), which limits the application of this section.

115. *Subsection (2)* explains that the Secretary of State imposes obligations on particular providers by the service of individual notices describing in much greater detail than the order the precise steps they are required to take.

As to what steps may be imposed, see subsections (3) and (11). For the time limits for compliance, see subsection (8).

116. *Subsection (4)* provides that commercial and other organisations which provide a telecommunications service as no more than a means of accessing a further service of theirs (for example, a telephone banking service) will not be subject to any order under this section. The subsection also puts outside the scope of the section a telecommunications service that is necessarily incidental to a different service.

117. *Subsections (5) and (6)* concern the consideration of notices by the Technical Advisory Board (established by Section 13(1)). Where a person is served with a notice under subsection (2), they may ask the Board to consider the notice. The Board will consider the technical requirements and financial consequence of the notice, and report their conclusions to the person on whom the notice was served and to the Secretary of State. During that time, the obligations under the notice are suspended by virtue of paragraph (a). The Secretary of State, on receipt of advice from the Board, may withdraw the notice or re-issue it with or without modifications.

118. *Subsection (7)* requires persons served with a notice under subsection (2) to comply with it. The Secretary of State may bring civil proceedings to enforce this duty.

119. *Subsection (9)* requires the Secretary of State to consult with a number of people prior to making an order. These include, as the Secretary of State considers appropriate, the persons likely to have obligations imposed on them and their representatives, the Technical Advisory Board, and bodies which have statutory functions affecting providers of communication services. The latter category includes, for example, OFTEL.

120. *Subsection (11)* explains that the steps that may be required to be taken should take account of the need for security and confidentiality and the need to facilitate (such as by audit mechanisms) the job of the Interception Commissioner.

Section 13: Technical Advisory Board

121. This Section provides for the establishment by order of a Technical Advisory Board. Its make-up will be prescribed by order (affirmative resolution – see subsection (3)), and must include a balanced representation of the interests of communications service providers and of those people listed in section 6(2).

Section 14: Grants for interception costs

122. This Section requires the Secretary of State to ensure that there are arrangements to secure that communications service providers receive such a contribution as is fair in each particular case to the costs of providing an intercept capability or in the provision of assistance in respect of individual warrants.

Section 15: General safeguards

123. This Section has the effect of restricting the use of intercepted material to the minimum necessary for the authorised purposes. Section 82(6) contains a transitional provision applying the provisions of Sections 15 and 16 to warrants and certificates under the 1985 Act.

124. *Subsection (1)* imposes a duty upon the Secretary of State to ensure that safeguard arrangements are in place to ensure the requirements of this section and section 15 are complied with.

125. *Subsection (2)* requires that the distribution and disclosure of intercepted material and related communications data are kept to a minimum.

126. *Subsection (3)* requires that all copies of any intercepted material and related communications data must be destroyed as soon it is no longer necessary to retain it for any of the authorised purposes (see below). This does not impose any obligation to retain material, which may therefore be destroyed earlier in some cases.