1. A request may only be made by the Intelligence Services to the government of a country or territory outside the United Kingdom for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual legal assistance agreement, if either:

a. a relevant interception warrant under the Regulation of Investigatory Powers Act 2000 ("RIPA") has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the communications at issue because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the Intelligence Services to obtain those communications; or

b. making the request for the communications at issue in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise contravene the principle established in *Padfield v. Minister of Agriculture, Fisheries and Food* [1968] AC 997 (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the Intelligence Services to obtain those communications.

For these purposes a "relevant RIPA interception warrant" means either (i) a s8(1) warrant in relation to the target at issue; (ii) a s8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" (within the meaning of s8(4)(b) of RIPA) covering the target's communications, together with an appropriate s16(3) modification (for individuals known to be within the British Islands); or (iii) a s8(4) warrant and accompanying certificate which includes one or more "descriptions of intercepted material" covering the target's communications (for other individuals). The reference to a "*warrant for interception, signed by a Minister*" being "*already in place*" in the ISC's Statement of 17 July 2013 should be understood in these terms. (Given sub-paragraph (b), and as previously submitted in open, a RIPA interception warrant is not as a matter of law required in all cases in which unanalysed intercepted communications might be sought from a foreign government.)

2. Where the Intelligence Services receive unanalysed intercepted communications content and associated communications data from the government of a country or territory outside the United Kingdom (whether solicited or unsolicited), those communications and communications data are – pursuant to internal "arrangements" – subject to the same internal rules and safeguards as selected

communications content and related communications data that are obtained directly by the Intelligence Services as a result of interception under RIPA. For these purposes, "selected communications content" means communications content resulting from interception under a s8(1) warrant, or from the selection processes that are applied, pursuant to s16 of RIPA, to communications obtained under a s8(4) warrant.

3. Those of the Intelligence Services that receive unanalysed intercepted material and related communications data from an interception under a s8(4) warrant have internal "arrangements" that require a record to be created, explaining why access to the unanalysed intercepted material is required, before an authorised person is able to access such material pursuant to s16 of RIPA.

4. The internal "arrangements" of those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s8(4) warrant specify (or require to be determined, on a system-by-system basis) maximum retention periods for different categories of such data which reflect the nature and intrusiveness of the particular data at issue. The periods so specified (or determined) are normally no longer than two years, and in certain cases are significantly shorter (intelligence reports that draw on such data are treated as a separate category, and are retained for longer). Data may only be retained for longer than the applicable maximum retention period where prior authorisation has been obtained from a senior official within the particular Intelligence Service at issue on the basis that continued retention of the particular data at issue has been assessed to be necessary and proportionate (if the continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, such data are deleted). As far as possible, all retention periods are implemented by a process of automated deletion which is triggered once the applicable maximum retention period has been reached for the data at issue. The maximum retention periods are overseen by, and agreed with, the Interception of Communications Commissioner.

5. The intelligence services' internal "arrangements" under the Security Service Act 1989 / the Intelligence Services Act 1994 and s15-16 of RIPA are periodically reviewed to ensure that they remain up-to-date and effective. Further, the Intelligence Agencies are henceforth content to consider, during the course of such periodic reviews, whether more of those internal arrangements might safely and usefully be put into the public domain (for example, by way of inclusion in a relevant statutory code of practice).