SCHEDULE 5

Article 30

INFORMATION SECURITY ITEMS

1. In this Schedule—

"business or academic collaborator", in relation to an exporter, means a person who is either—

(a) working by way of business in research and development of cryptography or cryptographic goods or software; or

(b) is teaching, or undertaking research as a member of or at a university or institution of higher education into, cryptography or cryptographic goods or software,

and with whom the exporter has previously entered into a collaboration agreement;

"collaboration agreement" means an agreement for the carrying out of work comprising or related to research into the development of cryptography or cryptographic goods or software;

"development" has the same meaning as in Schedule 2;

"intra-group or collaborative end-use" means—

(a) use by the exporter, or a subsidiary undertaking or parent undertaking of the exporter, in that person's own commercial cryptographic goods; or

(b) use by a business or academic collaborator of the exporter in that person's own commercial cryptographic goods in accordance with the terms of a collaboration agreement with the exporter;

"parent undertaking" and "subsidiary undertaking" have the same meanings as in the Companies Act 2006(**1**) (see section 1162 of, and Schedule 7 to, that Act);

"production", "technology" and "use" have the same meanings as in Schedule 2.

2. The information security items specified in this Schedule are the following software and technology—

(a) cryptography development software specified in entry 5D002 of Annex I to the dual-use Regulation, other than software having the characteristics, or performing or simulating the functions, of equipment designed or modified to perform cryptanalytic functions;

(b) cryptography development technology specified in entry 5E002 of Annex I to the dual-use Regulation, other than technology for the development, production or use of—

(i) equipment designed or modified to perform cryptanalytic functions; or

(ii) software having the characteristics, or performing or simulating the functions, of equipment designed or modified to perform cryptanalytic functions

but only to the extent that such software or technology is for an intra-group or collaborative end-use.

3. The information specified in this Schedule is—

(a) a general description of the goods, software or technology, such as might be contained in a product brochure;

(b) descriptions of all relevant encryption algorithms and key management schemes, and descriptions of how they are used by the goods, software or technology (eg, which algorithm is used for authentication, which for confidentiality and which for key exchange); and details (eg, source code) of how they are implemented (eg, how keys are generated and distributed, how key length is governed and how the algorithm and keys are called by the software);

(**1**) 2006 c. 46.

(c) details of any measures taken to preclude user modification of the encryption algorithm, key management scheme or key length;

(d) details of pre- or post-processing of data, such as compression of plain text or packetisation of encrypted data;

(e) details of programming interfaces that can be used to gain access to the cryptographic functionality of the goods, software or technology; and

(f) a list of any protocols to which the goods, software or technology adhere.