

SCHEDULE 5

INFORMATION SECURITY ITEMS

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);
- (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.