SCHEDULE

OBLIGATIONS ON SERVICE PROVIDERS

Part II: Interception Capability for Public Telecommunication Services

5. To provide a mechanism for implementing interceptions within one working day of the service provider being informed that the interception has been appropriately authorised.

6. To ensure the interception, in their entirety, of all communications and related communications data authorised by the interception warrant and to ensure their simultaneous (i.e. in near real time) transmission to a hand-over point within the service provider's network as agreed with the person on whose application the interception warrant was issued.

7. To ensure that the intercepted communication and the related communications data will be transmitted so that they can be unambiguously correlated.

8. To ensure that the hand-over interface complies with any requirements communicated by the Secretary of State to the service provider, which, where practicable and appropriate, will be in line with agreed industry standards (such as those of the European Telecommunications Standards Institute).

9. To ensure filtering to provide only the traffic data associated with the warranted telecommunications identifier, where reasonable.

10. To ensure that the person on whose application the interception warrant was issued is able to remove any electronic protection applied by the service provider to the intercepted communication and the related communications data.

11. To enable the simultaneous interception of the communications of up to 1 in 10,000 of the persons to whom the service provider provides the public telecommunications service, provided that those persons number more than 10,000.

12. To ensure that the reliability of the interception capability is at least equal to the reliability of the public telecommunications service carrying the communication which is being intercepted.

13. To ensure that the intercept capability may be audited so that it is possible to confirm that the intercepted communications and related communications data are from, or intended for the interception subject, or originate from or are intended for transmission to, the premises named in the interception warrant.

14. To comply with the obligations set out in paragraphs 5 to 13 above in such a manner that the chance of the interception subject or other unauthorised persons becoming aware of any interception is minimised.