TAB

Technical Advisory Board

FIRST ANNUAL REPORT

1 APRIL 2002 TO 31 MARCH 2003

CONTENTS

FOREWORD

I am delighted to introduce the first Annual Report of the Technical Advisory Board, covering its work since inception.

The Board was established under the Regulation of Investigatory Powers Act 2000 which requires communication service providers to maintain a reasonable interception capability in order to safeguard national security and help fight organised crime. Its role and how this is discharged are brought out more fully in the body of the report.

I believe the Board's creation is an important one for several reasons. Firstly, as a body representing the interests of both the intercepting agencies and the communications industry, it provides a fundamentally fair approach to dealing with the issues referred to it. By its very existence it should give reassurance to the wider communications industry that the government is committed to working with communications service providers rather than simply imposing demands on them. I am convinced that it is through this type of consultation and co-operation that effective solutions are found.

In the initial phase of our work we have helped to define the general obligations government expects of communications service providers in the field of interception. We now stand ready to examine cases referred to us should individual communications service providers feel the notices defining their individual obligations are unfair.

The work of the Technical Advisory Board has potentially far reaching consequences for our society as a whole. At a time government is actively seeking to balance the protection of national security and preventing or detecting serious crime with safeguarding the privacy of the individual the Technical Advisory Board has a vital part to play.

LIAM STRONG

CHAPTER 1

FUNCTION OF THE TECHNICAL ADVISORY BOARD

Role of the Board

1.1 The Technical Advisory Board is an advisory non-departmental public body which was established in May 2002 under section 13 of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Regulation of Investigatory Powers (Technical Advisory Board) Order 2001 which came into force on 22 November 2001. Its role is to provide advice to the Home Secretary on whether specific obligations to maintain an interception capability imposed on communications service providers (CSPs) are reasonable. In addition to the ongoing provision of advice in specific cases, the Board was consulted prior to the laying before Parliament of general advice to CSPs on these obligations. This general advice was contained in the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002.

Background to the setting up of the Board

1.2 Interception of communications is regulated by RIPA Section I Part I (see Chapter 5). Under RIPA the Secretary of State issues warrants to law enforcement or intelligence agencies which they may serve on the companies (CSPs) providing the particular communications service to be intercepted. Section 12 of RIPA provides for the Secretary of State to impose on CSPs obligations to ensure they are and remain able to provide an interception capability in order to give effect to interception warrants. The obligations are listed in the schedule to the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002. That order also describes categories of service providers to whom such obligations shall not apply.

1.3 The obligations in the order are imposed on a CSP by the giving of a notice requiring the CSP to take all such steps specified or described in it. Such steps include those needed to ensure security and confidentiality in relation to interception and those needed to facilitate the work of the Interception of Communications Commissioner. A notice given to a CSP will have been the product of prior discussion and negotiation between that CSP and representatives of the government.

Referral of notices to the Board

1.4 The Board fulfils its functions by convening meetings as required and at least once a year. If a CSP is given a notice under section 12 of RIPA and considers either the steps appearing in it, or their financial consequences, unreasonable, it can refer the notice to the Technical Advisory Board, outlining the reasons for the referral, within 28 days. The Board will then consider the notice and assess its reasonableness. If appropriate, the Chairman may seek expert advice from outside the Board. The Technical Advisory Board will then report to the Home Secretary and to the CSP making the referral. After considering any report from the Board, the Secretary of State may either withdraw the notice, or give a further notice confirming its effect, with or without modifications.

CHAPTER 2

MEMBERSHIP OF THE TECHNICAL ADVISORY BOARD

2.1 Members of the Board are appointed by the Home Secretary in accordance with section 13 of RIPA and the Regulation of Investigatory Powers (Technical Advisory Board) Order 2001. Appointments are made in accordance with the guidelines on Ministerial appointments to public bodies issued by the Office of the Commissioner for Public Appointments.

2.2 Members are appointed on a personal basis, for the skills and experience brought to the position. They are not chosen to represent particular communications service providers or intercepting agencies.

2.3 The Board consists of six representatives of the communications industry, six representatives of the intercepting agencies and a neutral Chairman, currently Liam Strong. The Chairman is responsible directly to the Home Secretary. The names of those representing the intercepting agencies are not made public, but the industry representatives are:

- Derek Cobb (presently of NTL);
- Jim Cottrell (presently of Energis2);
- Jessica Hendrie-Liano (presently of Beachcroft Wansbroughs);
- Tom Phillips (presently of Cable and Wireless);
- Mike Short (presently of O_2); and
- Robert Temple (presently of British Telecom).

2.4 Board members' role, professional conduct and standards are regulated by a published Code of Practice and Terms of Reference (see Appendices (i) and (ii)).

2.5 Board members are appointed initially for three years and are subject to re-appointment by the Home Secretary. Individual members can have their appointment terminated by the Home Secretary if they fail to perform the duties required of them in line with the standards expected of public office.

CHAPTER 3

COSTS AND PAYMENTS

3.1 The Board's sponsoring department is the Home Office. The Crime Reduction and Community Safety Group in the Home Office provides secretariat and administrative support and access to any policy or legal guidance the Board requires in discharging its functions.

3.2 All appointees to the Board are part-time. The Chairman's remuneration is £400 a day plus expenses; the members are remunerated for expenses only.

3.3 Remuneration for the Board's first year amounted to £1,365.62.

CHAPTER 4

MEETINGS HELD

4.1 The Board met on 20 May 2002, 19 July 2002 and 18 October 2002.

4.2 Key issues the Board has addressed itself to have included:

- the production of Terms of Reference and a Code of Practice;
- advice to the Home Secretary on the drafting the Regulation of Investigatory Powers (Maintenance of Interception Capability) order 2002;
- preparation of a mechanism for considering representations from communications service providers on their obligations to maintain an intercept capability;
- consideration of the likely costs incurred by communications service providers in complying with their intercept obligations;
- participation in steps to reduce the likelihood of communication service providers referring complaints to the Board, including guidance on the contents of notices served on them;
- the setting up of a Technical Advisory Board website.

4.3 No Section 12 notices were referred to the Board during 2002-2003.

CHAPTER 5

BACKGROUND: REGULATION OF INVESTIGATORY POWERS ACT 2000

5.1 The Regulation of Investigatory Powers Act 2000 (RIPA) repealed the Interception of Communications Act 1985 (IOCA). It came into force on 2 October 2000, on the same day as the coming into force of the Human Rights Act 1998 which incorporated the European Convention on Human Rights (ECHR) into UK law. RIPA brought about a number of changes in the law and the practice of those responsible for the lawful interception of communications, deployment of covert surveillance and use of human intelligence sources.

5.2 Interception of communications is regulated by Section I Part I of RIPA. This allows the Secretary of State to issue warrants to intercepting agencies for the interception of the communications of people who are being investigated on the grounds given at 5.4 below. The agencies may then request the assistance of those companies providing the communications service, whether postal, internet, landline or mobile phone in order to give effect to the warrant. Under RIPA, companies providing communications services may be required to maintain a permanent interception capability. This requirement is imposed by the giving of one or more notices issued by the Secretary of State under section 12 of RIPA.

5.3 The persons that may apply to the Secretary of State for an interception warrant are:

- the Chief of the Secret Intelligence Service (MI6);
- the Director General of the Security Service (MI5);
- the Director of the Government Communications Headquarters (GCHQ);
- the Director General of the National Criminal Intelligence Service;
- the Commissioner of Police of the Metropolis;
- the Chief Constable of the Police Service of Northern Ireland;
- the chief constable of any Scottish police force;
- the Commissioners of HM Customs and Excise; and
- the Chief of Defence Intelligence.

5.4 There are three grounds on which a warrant can be sought:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime; or
- for the purpose of safeguarding the economic well-being of the United Kingdom.

5.5 Interception warrants specify either a person or a single set of premises as the interception subject, and include a schedule or schedules listing the addresses or telephone numbers that the agency wishes to intercept in relation to it. In considering whether to issue an interception warrant the Secretary of State must judge whether the information sought is necessary or could reasonably be

acquired by other means. He must also believe that the conduct authorised by the warrant is proportionate to what it seeks to achieve.

5.6 All warrants are valid for an initial period of three months. On renewal, warrants applied for on national security or economic well-being grounds would be valid for a further six months or three months for serious crime warrants.

Interception Commissioner

5.7 The current oversight and redress procedures include the appointment of an Interception Commissioner to oversee the Secretary of State's use of his power to issue interception warrants under RIPA and its related Codes of Practice. The Interception Commissioner, currently Sir Swinton Thomas, can require any person involved in the interception of communications to disclose any documents or information as he may require for carrying out his functions. Sir Swinton Thomas is a retired court of appeal judge. His annual report to the Prime Minister is published. The most recent annual report stated that the Home Secretary issued 1,314 warrants in 2001.

CHAPTER 6

CONTACT AND FURTHER INFORMATION DETAILS

6.1 Referrals or requests for further information should be made to:

The Technical Advisory Board
PO Box 38542
London SW1H 9YE

6.2 E-mails can be addressed to:

TAB@homeoffice.gsi.gov.uk

6.3 The Technical Advisory Board website is at:

http://security.homeoffice.gov.uk/ripa/interception/technical-advisory-board/

APPENDIX I

TAB

Technical Advisory Board

TERMS OF REFERENCE FOR

THE TECHNICAL ADVISORY BOARD

First Edition 2002

TERMS OF REFERENCE FOR THE TECHNICAL ADVISORY BOARD

Legislative basis for the Technical Advisory Board (TAB)

1. The Technical Advisory Board, hereafter referred to as the TAB, is an advisory Non-Departmental Public Body established by section 13(1) of the Regulation of Investigatory Powers Act 2000, hereafter referred to as the 2000 Act.

Role and purpose

2. The TAB has two functions.

- In accordance with section 12(9) of the 2000 Act, the TAB must be consulted before the Home Secretary makes an order under section 12(1) of the 2000 Act, imposing obligations on communications service providers (CSPs).

- In accordance with section 12(5) of the 2000 Act, a notice issued to a CSP under section 12(2), the effect of which is to trigger the imposition of the obligations provided for in the section 12(1) order, may be referred by the CSP to the TAB within 28 days of the notice's issue. In accordance with section 12 (6), the TAB shall consider the requirements set out in the notice and their financial consequences for the CSP. It shall then report its views to the CSP and to the Home Secretary. After considering any report from the TAB relating to a notice, the Home Secretary may either withdraw the notice or give a further notice under section 12(2) of the 2000 Act confirming its effect, with or without modifications.

Working practices

3. The TAB will fulfill its functions by convening meetings when required, but at least once a year. It will give careful consideration to the matters brought before it, where appropriate seeking evidence and expert advice from outside its own membership. The TAB chairman shall report the TAB's conclusions, in writing, to the Home Secretary. In relation to a notice issued under section 12(2) of the 2000 Act and referred to the TAB for consideration, the TAB chairman shall also report its conclusions, in writing, to the person making the reference. The TAB will operate business practices that meet its objectives within legislation concerning the management of data and the provision of access to information. The TAB chairman will publish an annual report and ensure that the TAB communicates effectively with both CSPs and the general public.

Membership

4. The membership of the TAB is provided for by the Regulation of Investigatory Powers (Technical Advisory Board) Order 2001. There shall be 13 members. Six industry members (holding an office, rank or position with a CSP, or with a body representing the interests of CSPs) and six government members (holding office, rank or position with an intercepting agency, or with a body representing their interests). One person, who does not fall within either of the previous two categories, shall be appointed chairman.

Recruitment of TAB members

5. Recruitment of the TAB chairman and industry members shall be conducted in accordance with the guidelines on ministerial appointments to public bodies issued by the Office for the Commissioner for Public Appointments (OCPA). The government members shall be nominated by the intercepting agencies and appointed by the Home Secretary.

Responsibilities of the TAB chairman

6. The chairman is responsible for chairing and managing the work of the TAB. He or She must also ensure that the TAB operates within the parameters set out in the Cabinet Office's "Non-Departmental Public Bodies: A Guide for Departments". The chair is directly responsible to the Home Secretary. His or Her key tasks and objectives are:

- participating in the recruitment of TAB industry members;
- leading the work of the TAB in the production of advice for the Secretary of State;
- producing an annual report on the TAB's activities;
- reviewing the appointment of TAB members every 3 years and making recommendations to the Secretary of State;
- ensuring that the TAB is able to call on appropriate experts as and when required;
- agreeing a code of practice for TAB members with the head of the sponsoring Home Office Unit (the Intelligence and Security Liaison Unit), ensuring that the code of practice is, where practicable and appropriate, consistent with Cabinet Office guidelines and reporting any breaches of the code of practice to the Home Secretary.

Responsibilities of TAB members

7. TAB members are responsible to the TAB chairman, assisting him or her to formulate advice for the Secretary of State on matters referred to the TAB for consideration. TAB members must at all times abide by the TAB's code of practice.

Terms and conditions for the post of TAB chairman

8. The terms and conditions for the post of TAB chairman are as follows:

- the post holder will need to be developed vetted;
- the post holder will need to abide by the code of practice for TAB members;
- the post holder cannot be a current employee of a communication service provider or an intercepting agency;
- the remuneration is £400 per day plus expenses. The initial appointment is for three years with the possibility of renewal.

Terms and conditions for the post of TAB member

9. The terms and conditions for the post of TAB member are:

- the post holder will need to be vetted to at least security check level;
- the post holder will need to abide by the code of practice for TAB members;
- no remuneration will be received, but expenses will be reimbursed. Appointments will be for three years with the possibility of renewal.

TAB secretariat and relationship with the Home Office

10. The Home Office will provide the TAB with a secretary, administrative support and any policy or legal guidance it requires. The Home Office will also administer TAB members' expense claims and payments to the TAB chairman, and act as a conduit between the TAB and other Government Departments and Agencies, as required.

Review of the functions of the TAB

11. The TAB chairman should review the functions of the TAB on a quinquennial basis, in line with Cabinet Office guidance.

Contacting the TAB

12. The TAB may be contacted by writing to The Technical Advisory Board, PO Box 38542, London SW1H 9YE. Alternatively, e-mails may be addressed to **TAB@homeoffice.gsi.gov.uk.**

13. The TAB homepage, which provides further information on the TAB, including copies of both this document and the TAB's Code of Practice, can be found at http://security.homeoffice.gov.uk/ripa/interception/technical-advisory-board/

APPENDIX II

TAB

Technical Advisory Board

CODE OF PRACTICE FOR MEMBERS OF

THE TECHNICAL ADVISORY BOARD

First Edition 2002

CODE OF PRACTICE FOR MEMBERS OF THE TECHNICAL ADVISORY BOARD[1]

Public service values

1. The members of the Technical Advisory Board, hereafter referred to as the TAB, must at all times:

   - observe the highest standards of impartiality, integrity and objectivity in relation to the advice they provide and the management of the TAB;

   - be accountable to Parliament and the public more generally for its activities and for the standard of advice it provides; and

2. The TAB will operate business practices that meet its objectives within legislation concerning the management of data and the provision of access to information. Much of the TAB's work will be of a sensitive nature and its membership includes representatives of the intercepting agencies. It is not, therefore, appropriate for the TAB to meet in public. Neither is it appropriate for the identities of those TAB members representing the intercepting agencies to be made public. For this reason, while the TAB chairman will maintain a register of interests, only details pertaining to the chairman and industry members will be made publicly available on request.

3. The Home Secretary is answerable to Parliament for the policies and performance of the TAB, including the policy framework within which it operates.

Standards in Public Life

4. All TAB members must:

   - follow the Seven Principles of Public Life set out by the Committee on Standards in Public Life (annexed);

   - comply with this Code of Practice for Members of the TAB, and ensure they understand their duties, rights and responsibilities, and that they are familiar with the function and role of the TAB and any relevant statements of Government policy. New TAB members should consider attending relevant training or induction courses.

   - not misuse information gained in the course of their public service for personal gain or for political purpose, nor seek to use the opportunity of

[1] An advisory non-departmental public body established in accordance with section 13 of the Regulation of Investigatory Powers act 2000 and sponsored by the Intelligence and Security Liaison Unit

public service to promote their private interests or those of connected persons, firms, businesses or other organisations; and

- not hold any paid or high-profile unpaid posts in a political party, and not engage in specific political activities on matters directly affecting the work of this body. When engaging in other political activities, TAB members should be conscious of their public role and exercise proper discretion. These restrictions do not apply to MPs, to local councillors, or to Peers in relation to their conduct in the House of Lords.

Role of the TAB members

5. TAB members have collective responsibility for the operation of the TAB. They must:

- engage fully in collective consideration of the issues, taking account of the full range of relevant factors, including any guidance issued by the sponsor department or the responsible Minister;

- operate business practices that meet the TAB's objectives within legislation concerning the management of data and the provision of access to information. (including prompt responses to public requests for information) and agree an Annual Report;

- take responsibility for the security and protection of any sensitive or protectively marked information, documents and assets to which they gain access in the course of exercising their TAB functions;

- respond appropriately and in a timely manner to complaints, if necessary with reference to the Home Office; and

- ensure that the TAB does not exceed its powers or functions.

6. Communications between the TAB and the Home Secretary will generally be through the chair except where the TAB has agreed that an individual member should act on its behalf. Nevertheless, any TAB member has the right of access to Ministers on any matter which he or she believes raises important issues relating to his or her duties as a TAB member. In such cases the agreement of the rest of the TAB should normally be sought.

7. Communications between the TAB and communications service providers or members of the general public will, in general, also be conducted through the chair except where the TAB has agreed that an individual member should act on its behalf.

8. Individual TAB members can be removed from office by the Home Secretary if they fail to perform the duties required of them in line with the standards expected in public office.

The role of the chair

9. The chair has particular responsibility for providing effective leadership on the issues above. In addition, the chair is responsible for:

- ensuring that the TAB meets at appropriate intervals, and that the minutes of meeting and any reports to the Home Secretary accurately record the decisions taken and, where appropriate, the views of individual board members;

- ensuring that the TAB communicates effectively with government departments and agencies, communications service providers and the general public; and

- ensuring that new TAB members are briefed on appointment (and their training needs considered) and providing an assessment of their performance, on request, when members are considered for re-appointment to the TAB or for appointment to the board of some other public body.

Handling conflicts of interests

10. The purpose of these provisions is to avoid any danger of TAB members being influenced, or appearing to be influenced, by their private interests in the exercise of their public duties. TAB members should therefore declare any personal or business interest that may, or may be *perceived* (by a reasonable member of the public) to, influence their judgement. This should include, as a minimum, personal direct and indirect pecuniary interests, and should normally also include, such interests of close family members and of people living in the same household[2]. The register of interests should be kept up-to-date and those details pertaining to members who are not serving Crown or Civil Servants should be open to the public. A declaration of any interest should also be made at any TAB meeting if it relates specifically to a particular issue under consideration, for recording in the minutes (whether or not a TAB member also withdraws from the meeting).

11. TAB members should not participate in the discussion or determination of matters in which they have an interest, and should normally withdraw from the meeting if:

- their interest is direct and pecuniary; or

- their interest is covered in specific guidance issued by this body or the sponsor department which requires them not to participate and/or to withdraw from the meeting.

---

[2] Indirect pecuniary interests arise from connections with bodies which have a direct pecuniary interest or from being a business partner of, or being employed by, a person with such an interest. Non-pecuniary interests include those arising from membership of clubs and other organisations. Close family members include personal partners, parents, children (adult and minor), brothers, sisters and the personal partners of any of these.

Personal liability of board members

12. Legal proceedings by a third party against individual board members of advisory bodies, such as the TAB, are very exceptional. An individual member of the TAB who has acted honestly and in good faith will be indemnified in respect of the costs of defending any claim arising out of the execution or purported execution of his or her TAB functions and will not have to meet out of his or her personal resources any personal civil liability or liability to legal costs or expenses incurred in such execution or purported execution, except where his or her conduct goes beyond negligence and amounts to recklessness.

Annex

THE SEVEN PRINCIPLES OF PUBLIC LIFE

Selflessness

Holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends.

Integrity

Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisation that might influence them in the performance of their official duties.

Objectivity

In carrying out public business, including making public appointments, awarding contracts, or recommending individuals for rewards and benefits, holders of public office should make choices on merit.

Accountability

Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.

Openness

Holders of public office should be as open as possible about all the decisions and actions that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands.

Honesty

Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interests.

Leadership

Holders of public office should promote and support these principles by leadership and example.

APPENDIX III

STATUTORY INSTRUMENTS

2001 No. 3734
INVESTIGATORY POWERS

The Regulation of Investigatory Powers (Technical Advisory Board) Order 2001

Made	*21st November 2001*
Coming into force	*22nd November 2001*

Whereas a draft of this Order has been laid before Parliament and approved by a resolution of each House:

Now, therefore, the Secretary of State, in exercise of the powers conferred on him by section 13(1) and (2) of the Regulation of Investigatory Powers Act 2000[1], hereby makes the following Order:

Citation, commencement and interpretation
1. - (1) This Order may be cited as the Regulation of Investigatory Powers (Technical Advisory Board) Order 2001 and shall come into force on the day after the day on which it is made.

(2) In this Order, "the 2000 Act" means the Regulation of Investigatory Powers Act 2000.

Membership of the Board
2. - (1) The Technical Advisory Board established by section 13(1) of the 2000 Act shall consist of 13 persons.

(2) Of that number one person, who does not fall within paragraph (3), shall be appointed chairman.

(3) Of the remaining number -

(a) six shall be persons holding an office, rank or position with either -

(i) a person on whom obligations may be imposed under section 12 of the 2000 Act, or

(ii) a body representing the interests of such persons, and

(b) six shall be persons holding an office, rank or position with either -

(i) a person by or on whose behalf applications for interception warrants may be made, or

(ii) a body representing the interests of such persons.

Bob Ainsworth
Parliamentary Under-Secretary of State

Home Office
21st November 2001

EXPLANATORY NOTE

(This note is not part of the Order)

This Order provides for the membership of the Technical Advisory Board, established by section 13 of the Regulation of Investigatory Powers Act 2000 (c. 23).

The Board must be consulted before the Secretary of State makes an order under section 12(1) of the Act, imposing obligations on persons who are providing public postal services or public telecommunications services, or who are proposing to do so. The Board also has functions under section 12(6) of the Act, relating to the consideration of notices issued to service providers under section 12(2), the effect of which is to trigger the imposition of the obligations provided for in the section 12(1) order.

APPENDIX IV

STATUTORY INSTRUMENTS

2002 No. 1931
INVESTIGATORY POWERS
The Regulation of Investigatory Powers
(Maintenance of Interception Capability) Order 2002

Made	*22nd July 2002*
Coming into force	*1st August 2002*

Whereas the Secretary of State has consulted the persons listed in section 12(9) and (11) of the Regulation of Investigatory Powers Act 2000[1] about this Order;

And whereas a draft of this Order has been laid before Parliament and approved by a resolution of each House;

Now, therefore, the Secretary of State, in exercise of the powers conferred on him by section 12(1), (2) and (5) and section 78(5) of that Act, hereby makes the following Order:

Citation, commencement and interpretation
1. - (1) This Order may be cited as the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 and shall come into force on 1st August 2002.

(2) In this Order "service provider" means a person providing a public postal service or a public telecommunications service, or proposing to do so.

Interception capability
2. - (1) The Schedule to this Order sets out those obligations which appear to the Secretary of State reasonable to impose on service providers for the purpose of securing that it is and remains practicable for requirements to provide assistance in relation to interception warrants to be imposed and complied with.

(2) Subject to paragraph (3) the obligations in -

(a) Part I of the Schedule only apply to service providers who provide, or propose to provide, a public postal service; and

(b) Part II of the Schedule only apply to service providers who provide, or propose to provide, a public telecommunications service.

(3) The obligations in Part II of the Schedule shall not apply to service providers who -

(a) do not intend to provide a public telecommunications service to more than 10,000 persons in any one or more parts of the United Kingdom and do not do so; or

(b) only provide, or propose to provide, a public telecommunications service in relation to the provision of banking, insurance, investment or other financial services.

Interception capability notices

3. - (1) The Secretary of State may give a service provider a notice requiring him to take all such steps falling within paragraph (2) as may be specified or described in the notice.

(2) Those steps are ones appearing to the Secretary of State to be necessary for securing that the service provider has the practical capability of meeting the obligations set out in the Schedule to this Order.

Referral of notices to the Technical Advisory Board

4. The period within which any person to whom a notice has been given under article 3 may refer the notice to the Technical Advisory Board is specified as being before the end of 28 days from the date of the notice.

Bob Ainsworth
Parliamentary Under-Secretary of State

Home Office
22nd July 2002

SCHEDULE

Article 2
OBLIGATIONS ON SERVICE PROVIDERS

Part I: Interception Capability for Public Postal Services

1. To ensure the interception and temporary retention of postal items destined for addresses in the United Kingdom for provision to the person on whose application the interception warrant was issued.

2. To provide for the interception and retention of postal items sent by identified persons where the carrier keeps records of who sent which item in the course of their normal business.

3. To maintain a system of opening, copying and resealing of any postal item carried for less than £1.

4. To comply with the obligations set out in paragraphs 1 to 3 above in such a manner that the chance of the interception subject or other unauthorised persons becoming aware of any interception is minimised.

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.

EXPLANATORY NOTE

(This note is not part of the Order)

Part I of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act") contains provisions about the interception of communications transmitted by means of public postal service or a public telecommunications service. Interception is permitted under the 2000 Act by certain public authorities who obtain an interception warrant. This Order sets out the obligations which it appears to the Secretary of State reasonable to impose on the providers of public postal services or a public telecommunications services ("service providers") for the purpose of securing that it is and remains practicable for requirements to provide assistance in relation to interception warrants to be imposed and complied with.

These obligations are set out in the Schedule to the Order. The obligations in Part I of the Schedule relate only to persons who provide, or propose to provide, a public postal service. The obligations in Part II of the Schedule relate only to persons who offer, provide, or propose to provide a public telecommunications service to more than 10,000 persons in any one or more parts of the United Kingdom, other than service providers who only provide a public telecommunications service in relation to the provision of banking, insurance, investment or other financial services.

Article 3 enables the Secretary of State to ensure compliance with the obligations by providing that he may give a service provider a notice requiring it to take the steps described in the notice. The notice may only contain steps which appear to the Secretary of State necessary for securing that that service provider has the practical capability of meeting those obligations set out in the Schedule which apply to that service provider.

Article 4 specifies the period within which a person served with a notice may refer it to the Technical Advisory Board.

This Order was notified in draft to the European Commission in accordance with Directive 98/34/EC, as amended by Directive 98/48/EC.