ICT SERVICES AGREEMENT SCHEDULES

SCHEDULE 2.5

SECURITY REQUIREMENTS AND PLAN

CONTENTS

Section A

Product Description

1. PRODUCT TITLE

ICT Services Agreement - Schedule 2.5 (Security Requirements and Plan).

2. PURPOSE OF PRODUCT

To specify the principles of the security to be applied in providing the Services and to set out the key elements of, and the procedure for further developing, the security plan for the Services.

3. COMPOSITION

- Scope & Definition
- Principles of Security
- Security Plan
- Audit & Testing
- Compliance with ISO 27000
- Breach of Security

4. DERIVATION

Authority requirements and Security Policy

5. RELATED CLAUSES & SCHEDULES

Clauses: 9 (Services)

48 (Security Requirements)

55.1.5.5(d) (Termination for Cause by the Authority)

Guidance: Guidance Note 1 (Key Commercial Principles), section 1 - 7.1 (IPR in Specially Written Software) and 12 (Termination Events for Contractor Default)

Schedules: 2.3 (Standards)

4.1. (Contractor Solution)

6. ALLOCATION

Authority to submit draft schedule 2.5 to bidders during procurement for discussion and agreement. Contractor to prepare Security Plan in accordance with the schedule.

7. QUALITY / REVIEW

Authority expertise: technical, project management, procurement.

Section B

Guidance

1. INTRODUCTION

Please refer to the OGC Toolkit for a general discussion of security issues in an ICT context.

The Authority needs to ensure that it sets out in the schedule the security principles and its security requirements in respect of the Services and clearly delineate between the obligations on the Authority and the specific responsibilities of the Contractor. The schedule should be drafted with appropriate technical input.

2. PHYSICAL SECURITY

The Authority should specify their requirements for physically protecting servers, data backups, access to Sites, Authority Premises, staff security clearances etc.

3. SYSTEMS BASED SECURITY

The Authority should describe their requirements for securing data, access to systems, password controls, user permissions, network protection, virus, software patches, firewalls, etc.

4. STANDARDS

The Contractor should be required to comply with the relevant ISO and BS security standards currently ISO 27000.

The Authority will need to identify and add any additional security measures, not catered for by these standards.

5. SECURITY PLAN

The Authority should set out in the schedule a clear process for agreeing the security plan.

6. AUDIT AND TESTING

The Authority should set out a description of the audit and testing process to be used for the security requirements.

7. ACTIONS IN THE EVENT OF A BREACH OF SECURITY

The schedule should set out what measures the parties should take in the event of a security breach.

Section C

Pro-Forma/Example Schedule

[Guidance: This section sets out example security provisions that may be included and developed (as appropriate) to meet the Authority's requirements.]

[Guidance: subject to the agreement of this schedule, the following definitions will need to be added to schedule 1.]

"Breach of Security"	the occurrence of unauthorised access to or use of the Authority Premises, the Sites, the Services, the Contractor System or any ICT or data (including the Authority's Data) used by the Authority or the Contractor in connection with this Agreement.
"Security Plan"	the Contractor's security plan prepared pursuant to paragraph 3 of schedule 2.5 (Security Requirements and Plan) an outline of which is set out in Appendix of schedule 2.5 (Security Requirements and Plan);
"Security Policy"	the Authority's security policy annexed to schedule 2.5 (Security Requirements and Plan) as updated from time to time;
"Security Tests"	shall have the meaning set out in paragraph 11.1 of schedule 2.5 (Security Requirements and Plan);

8. INTRODUCTION

8.1 This schedule covers:

8.1.1 principles of security for the Contractor System, derived from the Security Policy, including without limitation principles of physical and information security;

8.1.2 [wider aspects of security relating to the Service];

8.1.3 the creation of the Security Plan;

8.1.4 audit and testing of the Security Plan;

8.1.5 conformance to ISO/IEC17799:2000 (Information Security Code of Practice) and BS7799-2:2002 (Standard Specification); and

8.1.6 breaches of Security.

9. PRINCIPLES OF SECURITY

9.1 The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Sites and the security for the Contractor System. The Contractor also acknowledges the confidentiality of the Authority's Data.

9.2 The Contractor shall be responsible for the security of the Contractor System and shall at all times provide a level of security which:

9.2.1 is in accordance with Good Industry Practice and Law;

9.2.2 complies with the Security Policy;

9.2.3 meets any specific security threats to the Contractor System; and

9.2.4 complies with ISO/IEC17799:2000 and BS7799-2:2002 in accordance with paragraph 12 of this schedule.

9.3 Without limiting paragraph 9.2, the Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to maintain the following at acceptable risk levels (to be defined by the Authority):

9.3.1 loss of integrity of the Authority's Data;

9.3.2 loss of confidentiality of the Authority's Data;

9.3.3 unauthorised access to, use of, or interference with the Authority's Data by any person or organisation;

9.3.4 unauthorised access to network elements, buildings, [the Authority Premises,] [the Sites,] and tools used by the Contractor in the provision of the Services;

9.3.5 use of the Contractor System or Services by any third party in order to gain unauthorised access to any computer resource or data of the Authority; and

9.3.6 loss of availability of the Authority's Data due to any failure or compromise of the Services.

10. SECURITY PLAN

10.1 Introduction

10.1.1 The Contractor shall develop, implement and maintain a Security Plan to apply during the Term (and after the end of the Term (as applicable) in accordance with schedule 8.5 (Exit Management)) which will be approved by the Authority, tested, periodically updated and audited in accordance with this schedule.

10.1.2 A draft Security Plan provided by the Contractor as part of its bid is set out in Appendix 2.

[***Guidance: Bidders should be obliged to provide a draft security policy as part of their bid. They should be instructed to prepare it with the same objectives and contents as the final plan as required by this schedule***].

10.2 Development

10.2.1 Within 20 Days after the Effective Date and in accordance with paragraph 10.4 (Amendment and Revision), the Contractor will prepare

and deliver to the Authority for approval the full and final Security Plan which will be based on the draft Security Plan set out in Appendix 2.

10.2.2 If the Security Plan is approved by the Authority it will be adopted immediately. If the Security Plan is not approved by the Authority the Contractor shall amend it within [10] Working Days of a notice of non-approval from the Authority and re-submit to the Authority for approval. The parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than [15] Working Days (or such other period as the parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this paragraph 10.2.2 of this schedule may be unreasonably withheld or delayed. However any failure to approve the Security Plan on the grounds that it does not comply with the requirements set out in paragraphs 10.1.1 to 10.3.5 shall be deemed to be reasonable.

10.3 **Content**

10.3.1 The Security Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with:

10.3.1.1 the provisions of this schedule (including the principles set out in paragraph 2);

10.3.1.2 the provisions of schedule 2.1 (Services Description) relating to security;

10.3.1.3 ISO/IEC17799:2000 and [BS7799-2:2002];

10.3.1.4 the data protection compliance guidance produced by the Authority;

10.3.1.5 [appropriate ICT standards for technical countermeasures which are included in the Contractor System;] and

10.3.1.6 [encryption standards in accordance with S(E)N 02/3 from CESG].

10.3.2 The references to standards, guidance and policies set out in paragraph 10.3.1 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, from time to time.

10.3.3 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Contractor should notify the Authority's Representative of such inconsistency immediately upon becoming aware of the same, and the Authority's Representative shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.

10.3.4 The Security Plan will be structured in accordance with ISO/IEC17799:2000 and BS7799-2:2002, cross-referencing if necessary to other schedules of this Agreement which cover specific areas included within that standard.

10.3.5 The Security Plan shall be written in plain English in language which is readily comprehensible to the staff of the Contractor and the Authority engaged in the Services and shall not reference any other documents which are not either in the possession of the Authority or otherwise specified in this schedule.

10.4 **Amendment and Revision**

10.4.1 The Security Plan will be fully reviewed and updated by the Contractor annually, or from time to time to reflect:

10.4.1.1 emerging changes Good Industry Practice;

10.4.1.2 any change or proposed change to the Contractor System, the Services and/or associated processes; and

10.4.1.3 any new perceived or changed threats to the Contractor System.

10.4.1.4 a reasonable request by the Authority

10.4.2 The Contractor will provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the Security Plan at no additional cost to the Authority.

10.4.3 Any change or amendment which the Contractor proposes to make to the Security Plan (as a result of an Authority request or change to the Authority's Requirements or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Authority.

11. AUDIT AND TESTING

11.1 The Contractor shall conduct tests of the processes and countermeasures contained in the Security Plan (**"Security Tests"**) on an [annual] basis or as otherwise agreed by the parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority.

11.2 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Contractor shall provide the Authority with the results of such tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

11.3 Without prejudice to any other right of audit or access granted to the Authority pursuant to this Agreement, the Authority shall be entitled at any time and without giving notice to the Contractor to carry out such tests (including penetration tests) as it may deem necessary in relation to the Security Plan and the Contractor's compliance with and implementation of the Security Plan. The Authority may notify the Contractor of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the delivery Services. If such tests impact adversely on its ability to deliver the Services to the agreed Service Levels, the Contractor shall be granted relief against any resultant under-performance for the period of the tests.

11.4 Where any Security Test carried out pursuant to paragraphs 11.2 or 11.3 above reveals any actual or potential security failure or weaknesses, the Contractor shall promptly notify the Authority of any changes to the Security Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to the Authority's approval in accordance with paragraph 10.4.3, the Contractor shall implement such changes to the Security Plan in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Security Plan to address a non-compliance with the Security Policy or security requirements, the change to the Security Plan shall be at no additional cost to the Authority. For the purposes of this paragraph 11, a weakness means a vulnerability in security and a potential security failure means a possible breach of the Security Plan or security requirements.

12. COMPLIANCE WITH ISO 2700

12.1 [The Contractor shall obtain independent certification of the Security Plan to ISO 27000 as soon as reasonably practicable and will maintain such certification for the duration of the Agreement.]

12.2 [If certain parts of the Security Policy do not conform to good industry practice as described in ISO 27000 and, as a result, the Contractor reasonably believes that its certification to ISO 27000 would fail in regard to these parts, the Contractor shall promptly notify the Authority of this and the Authority in its absolute discretion may waive the requirement for certification in respect of the relevant parts.]

12.3 The Contractor shall carry out such regular security audits as may be required by the British Standards Institute in order to maintain delivery of the Services in compliance with security aspects of ISO 27000 and shall promptly provide to the Authority any associated security audit reports and shall otherwise notify the Authority of the results of such security audits.

12.4 If it is the Authority's reasonable opinion that compliance with the principles and practices of ISO 27000 is not being achieved by the Contractor, then the Authority shall notify the Contractor of the same and give the Contractor a reasonable time (having regard to the extent of any non-compliance and any other relevant circumstances) to become compliant with the principles and practices of ISO 27000.

If the Contractor does not become compliant within the required time then the Authority has the right to obtain an independent audit against these standards in whole or in part.

12.5 If, as a result of any such independent audit as described in paragraph 12.4 the Contractor is found to be non-compliant with the principles and practices of ISO 27000 then the Contractor shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Authority in obtaining such audit.

13. BREACH OF SECURITY

13.1 Either party shall notify the other immediately upon becoming aware of any Breach of Security including, but not limited to an actual, potential or attempted breach, or threat to, the Security Plan.

13.2 Upon becoming aware of any of the circumstances referred to in paragraph 13.1, the Contractor shall:

13.2.1 immediately take all reasonable steps necessary to:

13.2.1.1 remedy such breach or protect the Contractor System against any such potential or attempted breach or threat; and

13.2.1.2 prevent an equivalent breach in the future.

Such steps shall include any action or changes reasonably required by the Authority. In the event that such action is taken in response to a breach that is determined by the Authority acting reasonably not to be covered by the obligations of the Contractor under this Agreement, then the Contractor shall be entitled to refer the matter to the Change Control Procedure.

13.2.2 as soon as reasonably practicable provide to the Authority full details (using such reporting mechanism as may be specified by the Authority from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

APPENDIX 1

Outline Security Plan

[***Guidance: Attach the outline Security Plan here***].

APPENDIX 2

Security Policy

[***Guidance: Attach the Security Policy here***].