SCHEDULE K

SECURITY

CONTENTS

1 INTRODUCTION

1.1 This Schedule details the security requirements which the Contractor shall abide by for the provision of IDENT1. It gives a brief overview of the security requirements for the provision of Services under this Contract and sets out the responsibilities incumbent upon the Contractor in relation to all activities in support of the provision of the Services. These requirements therefore apply not only to the Services, but to the Contractor's procedures, staff, facilities and systems which are used in association with the provision of the Services. The Authority may, according to English Law and to Treaties between the United Kingdom and other Countries, from time to time amend this Schedule (or Schedule D (**Detailed Operational Requirements**)) and any associated annexes which will clarify, augment or supersede the provisions of this Schedule without recourse to Schedule L (**Change Control Procedures**). The Contractor, its subcontractors and agents shall adhere to the provisions of this Schedule and to any subsequent amendments or annexes.

1.2 The Requirements relating directly to the IDENT1 Service are set out in Schedule D (**Detailed Operational Requirements**).

1.3 Definitions

The Glossary of Terms attached at Annex K-1 applies to this Schedule K (**Security**) only.

2 BACKGROUND

2.1 This Contract requires the Contractor to hold UK Protectively Marked material (that is, material which is classified under the UK Government Protective Marking Scheme) according to the prescribed standards. The standard of protection prescribed varies with the level of protective marking.

2.2 The Contractor shall submit the IDENT1 Service to formal accreditation by the National Accreditor for Police Systems and achieve formal accreditation by that body. The Accreditor is responsible to the Police Information Assurance Board (PIAB), a sub-committee of the ACPO Information Management Business Area. Both the PIAB and ACPO IMBA have Scottish representation.

3 GUIDANCE ON THE SECURITY PRINCIPLES AND PROTECTIVE MARKING OF ASSETS FOR IDENT1

3.1 General Principles

3.1.1 These security aspects are based upon UK Government information protection and security guidelines, and are aligned with the security requirements for the Services, including those security requirements set out in Schedule D (**Detailed Operational Requirements**).

3.1.2 Disclosure of Protectively Marked Assets must be strictly in accordance with the 'Need to Know' principle. It must be confined to those Contractor employees whose access to the Assets is essential for the purpose of the Contract.

3.1.3 The Contractor shall obtain prior written approval of the Authority before any Protectively Marked documents, knowledge, information, data or hardware is released or passed to any third party, and in particular to any foreign government, organisation, company or individual.

3.2 Personnel Security

3.2.1 The Contractor shall warn individuals having access to Protectively Marked Assets against divulging them to any unauthorised party and shall inform individuals that the Official Secrets Acts 1911-1989 apply to them.

3.2.2 Unless otherwise agreed with the Authority the Contractor shall submit its entire staff nominated to work on IDENT1 for security vetting by the Authority. The Authority will endeavour to progress vetting applications in a timely manner, in association with the Government Department(s) responsible.

(a) The Contractor shall ensure that staff nominated to work on IDENT1 who need privileged access to (NAFIS), SAFR and IDENT1 operational Assets, namely systems administrators, key operational support staff and developers, have been security cleared to SC level before they take up duty in such roles.

(b) The Contractor shall ensure that staff nominated to work on IDENT1 who require access to certain Police Force's Information Technology installations, such as data centre or data communications rooms, have been security cleared to SC level before they take up duty in such roles.

(c) The Contractor shall ensure that staff nominated to work on IDENT1 who need access to certain Police Force establishments, other than access to areas as detailed in Clause 3.2.2(b) above, have been security cleared to CTC level in addition to the standard BC clearance level before they take up duty in such roles.

(d) The Contractor shall ensure that all other staff nominated to work on IDENT1 who are not covered by the provisions of Clauses 3.2.2(a), 3.2.2(b) and 3.2.2(c) above shall be cleared to BC level at a minimum before they take up duty on IDENT1.

3.3 Asset Classification

3.3.1 Material passed to the Contractor by the Authority will bear the Protective Marking appropriate to it.

3.3.2 All Assets provided by the Contractor in relation to the delivery of the IDENT1 Service shall be classified and Protectively Marked as follows:

(a) Assets which do not contain sensitive information, or which contain information which is already authorised to be in the public domain, should not be protectively marked. Optionally, for clarity, such assets may be marked NOT PROTECTIVELY MARKED.

(b) Assets which contain information which the Authority considers to be RESTRICTED, or which contain your proprietary technical or commercial information which you do not wish to be disclosed into the public domain, or the disclosure of which to unauthorised third parties would prejudice your tender or your competitive position, should be marked RESTRICTED.

(c) Assets which are protectively marked may additionally contain a descriptor where this helps to identify to others the nature of the sensitivity and the groups, roles or people to whom access to the information should be confined.

3.3.3 As an example, documents in relating to technical solutions, or pricing, should be protectively marked RESTRICTED, RESTRICTED – COMMERCIAL, RESTRICTED – CONTRACTS or RESTRICTED – IDENT1; whereas copies of public domain company financial statements or product brochures should not be protectively marked.

3.3.4 Should the Authority need to apply a protective marking of CONFIDENTIAL or above to any Assets, the Authority will inform the Contractor of appropriate instructions for managing such Assets. In the absence of such specific instructions, the aspects described in this Schedule shall apply by default.

3.3.5 The legacy protective marking of COMMERCIAL-IN-CONFIDENCE is equivalent to RESTRICTED – COMMERCIAL.

3.3.6 Documents which do not attract a protective marking should not be protectively marked, as this would impose unnecessarily onerous overheads upon all Parties; nor should documents be unnecessarily 'over classified' as this dilutes the value of the protective marking scheme.

3.3.7 Further information on protective marking is set out in the enclosed leaflet entitled "Handling of Protectively Marked Material – A Guide for Police Personnel (October 2001)".

3.4 Transmission within Company Premises

Protectively Marked Assets shall be transmitted within the Contractor's premises only in such a way as to ensure that no unauthorised person has access.

3.5 Use of Automated Processing Systems

The use of automated processing systems for the management of Protectively Marked IDENT1 and associated Assets shall be subject to approval and accreditation as part of the IDENT1 accreditation process as detailed in Clause 4 below by the National Accreditor for Police systems. Additionally physical site visits may be made as part of the Accreditation process by the Accreditor or authorised agents approved by the Authority. Where the Contractor provides the necessary assurance that the 'Need To Know' principle is being enforced, that any risk of compromise of Assets is being mitigated, then approval and/or accreditation will not be unreasonably withheld.

3.6 Use of Mobile or Home Working Computers

The Contractor shall use mobile or home working automated processing systems only as approved and accredited according to Clause 4 below. Any Contractor's mobile or home working computer used to process or store such information should not be transported outside of the UK without prior written approval of the Authority.

3.7 Transmission Outside Contractor's Premises

3.7.1 In addition to the use of CAPS approved cryptographic products, the Authority approves the use of the PGP V8.0 or later commercial cryptographic product for the protection of **RESTRICTED** Assets whilst in transit (including over the public internet) and in storage electronically.

3.7.2 The Contractor shall not transmit Protectively Marked information via IT networks or via the public internet in any other way without the prior written approval of the Authority.

3.8 Transmission Abroad

Subject to the provisions of the Data Protection Act 1998, the Authority authorises shipment of **RESTRICTED** assets outside the UK by first class mail, by overnight commercial delivery services or hand-carried (with courier certificate), where the material is double wrapped, with the protective marking shown on the inner wrapper but not however on the outer wrapper.

3.9 Loss

Any loss or compromise of Protectively Marked Assets by the Contractor, its subcontractors or agents shall be reported by the Contractor to the Authority without delay.

3.10 Destruction

As soon as they are no longer required, the Contractor shall return protectively marked operational Assets and document originals and master copies to the Authority. Protectively Marked non-operational Assets shall be destroyed by the Contractor in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding, tearing into small pieces or degaussing. Protectively Marked non-operational Assets which are not required by the Contractor but which cannot be destroyed in such a way shall be returned by the Contractor to the Authority.

3.11 Operational Assets

The Contractor shall treated all operational IDENT1 data, information and other Assets, including legacy NAFIS, SAFR and Police Service data, information and other Assets that do not possess an explicit Protective Marking, as **RESTRICTED**.

4 ACCREDITATION

4.1 The Contractor shall submit the IDENT1 Service and all supporting Contractor and subcontractor facilities to formal accreditation by the National Accreditor for Police Systems and obtain formal accreditation prior to TOR. Where appropriate, the Authority will take advice on this matter from CESG and the Security Service. Thereafter, the IDENT1 Service and all supporting Contractor and subcontractor facilities shall be submitted for and obtain accreditation at least once every two years or at such time as the Accreditor deems appropriate.

4.2 The Contractor shall conduct a formal Security Risk Assessment using a recognised risk assessment methodology such as CRAMM.

4.3 The Accreditation process shall be against extant HMG Information Assurance Policy, including, but not limited to, HMG IS 1-5.

4.4 The Accreditation process shall include an assessment against the ISO17799 standard. The Contractor shall undertake an analysis of its own premises, staff, sub-contractors and technical aspects as deemed appropriate by the Accreditor.

4.5 The Contractor shall supply all documents relevant to Accreditation and shall work closely with the Accreditor to achieve Accreditation. For the avoidance of doubt, the Accreditor will decide if a document shall be relevant to the Accreditation process.

4.6 The Contractor shall provide a single point of contact to which all security aspects will be referred in the first instance.

4.7 The Contractor shall submit the system to an independent IT Health Check prior to formal Accreditation; this shall be undertaken by a CESG CHECK approved consultant. The scope of the Health Check shall be determined by the Accreditor. For the avoidance of doubt, the requirement hereunder for a Health Check shall not replace the requirement as set out in Section 13.3 of the Non-Functional Requirements of Schedule D (**Detailed Operational Requirements**).

4.8 The Contractor shall provide to the Authority an Accreditation Document Set, the broad format of which should be taken from HMG IS2 and accompanying documents (as set forth in documents 49 to 56 of Schedule O (**Documentation**).

5 GUIDANCE ON PERSONNEL VETTING

5.1 The aim of personnel security vetting is to identify those persons who may pose a threat to security and thereby, to exclude them from access to valuable Government assets, particularly sensitive or protectively marked material and sensitive sites.

5.2 Personnel vetting requirements for IDENT1 can be roughly divided in two areas. One, where access to Protectively Marked material is required and two, in areas where Protectively Marked assets could be of use to criminals.

5.3 The vetting system in use by Government departments is detailed in HMG Manual of Protective Security (MoPS). The defined vetting levels are as follows:

5.4 Security Check (SC)

5.4.1 is carried out when regular access to **SECRET** or occasional access to **TOP SECRET** is involved;

5.4.2 involves a check of departmental records, where they exist, completion of a security questionnaire, a criminal record check, a credit check and a check against security records;

5.4.3 a subject interview may be carried out in a small proportion of cases;

5.4.4 is reviewed every ten (10) years; and

5.4.5 is reviewed after three (3) years for contractors.

5.5 Developed Vetting (DV)

5.5.1 is carried out only when long-term, frequent and uncontrolled access to **TOP SECRET** information or to equivalent operations is involved;

5.5.2 involves all the process carried out for the Security Check, if these have not been carried out already, has a subject interview and a field investigation, which will involve interviews with referees and current and previous supervisors; and

5.5.3 is reviewed at varying intervals, usually five (5) years initially and thereafter every seven (7) years. Reviews can he brought forward at any time at the discretion of the DSO (Departmental Security Officer). In the case of people under twenty-one (21), reviews may be annual.

5.6 Counter Terrorist Check (CTC):

5.6.1 is carried out where a building or site is considered to be at serious risk of terrorist attack and also where information, possibly not protectively marked, is held which may be of use to terrorists; and

5.6.2 involves the completion of a security questionnaire, a check of criminal and counter terrorist records and very occasionally a subject interview.

5.7 Basic Check (BC):

5.7.1 is the minimum requirement for access to **RESTRICTED** and **CONFIDENTIAL** material and for occasional access to **SECRET**, although in some agreed cases there will be additional requirements;

5.7.2 is not a security check as such but is a package of pre-employment checks designed to provide a level of assurance of probable reliability; and

5.7.3 involves a check of original personal documentation, such as passports, driving licences etc. and the taking up of several references.

The National Accreditor may, at his discretion, authorise the Contractor perform checks of Contractor staff equivalent to the Basic Check on behalf of the Authority.

5.8 Basic Check Enhanced (BC(E)):

5.8.1 is a Home Office enhanced check approved by Cabinet Office;

5.8.2 involves all the processes carried out for the Basic Check; and

5.8.3 involves a criminal record check.

ANNEX K-1

GLOSSARY OF DEFINITIONS

The defined terms below shall only apply to this Schedule.

Asset: any thing of value, either tangible or intangible, that is owned or used by an organisation or business, including documents and information, materials or equipment, cash, operating systems, employee knowledge and skills, etc.

Availability: the continuous or timely access to information, systems or physical assets by authorised individuals.

Compromise: an accidental or deliberate violation of asset CONFIDENTIALITY or loss of INTEGRITY or AVAILABILITY due to, for example, unauthorised disclosure, loss, theft, destruction, tampering and deliberate or accidental damage.

Confidentiality: the restriction of information and other valuable assets to authorised individuals.

Integrity: the maintenance of information systems and physical assets in their complete and usable form.

Protective Marking System: a method of assigning asset values to things to indicate an appropriate level of security or protection required. Assets may be marked physically, for example, within headers and footers on printed documents, or for risk management purposes, may be treated as if they are marked.

Protective Markings: RESTRICTED, CONFIDENTIAL, SECRET and **TOP SECRET** are standard terms used to convey the value levels of sensitive assets and the commensurate amount of protection required for them.

Risk: the combination of threat and vulnerability. The probability or likelihood of an attack succeeding or of damage being sustained as a result of compromise to an asset. An acceptable risk is simply the level of risk that the manager is prepared to accept.

Risk Analysis: the process of determining the likelihood of an asset being compromised by considering the vulnerabilities of the asset against the known threats to that asset.

Risk Management: the management process designed to reduce the risk of a successful attack to an acceptable level, and to limit damage resulting from the compromise of an asset or assets. This is achievable in several ways, for example, by acceptance of the risk; transference of part of the risk by providing insurance or by moving the assets to another site; by implementing protective security. The process necessarily involves a comprehensive analysis and assessment of the risks as a preliminary step. Risk management is a dynamic process that needs to be kept under regular review.

Security Control: a method, device or activity designed to provide a degree of protection.

Threat: the probability or likelihood of an attack or a potentially compromising event taking place. Where a threat is from a human source, it is influenced by such factors as the capability, resources and intentions of those involved, and the value or attractiveness and accessibility of the asset.

Vulnerability: a feature or characteristic of an asset which could be exploited in an attack, for example, a VDU which emits radiation, windows which could shatter scattering lethal splinters of glass in an explosion, something which makes an asset particularly susceptible to compromise in the event of a disaster, such as, sub-ground areas liable to flooding.