

OFFICIAL



Crown
Commercial
Service

The Home Office

- and -

I.F.F Research Limited

CONTRACT

relating to

RM5090-SO8043

Provision of Police Workforce Census

ORDER FORM**RM1086 MR130001 UKSBS Market Research Framework Agreement (Lot 4)****FROM**

Authority	Home Office
Service Address	2 Marsham Street, London SW1P 4DF
Invoice Address	Home Office Shared Service Centre HO Box 5015 Newport South Wales NP20 9BB Post-Room-Rescan@homeoffice.gsi.gov.uk
Contact Ref:	Name: Redacted Text Phone: Redacted Text e-mail: Redacted Text
Title	Provision of Police Workforce Census
Order Reference	RM5090-SO8043
Order Number	
Order Date	26/02/2015

TO

Provider:	I.F.F Research Ltd
For the attention of: E-mail Telephone number	Name: Redacted Text Phone: Redacted Text e-mail: Redacted Text

Address	Chart House Chart Street London N1 6DD
----------------	-------------------------------------------------

1. SERVICES REQUIREMENTS
<p>(1.1) Services [and Deliverables] Required:</p> <p>See Annex A for full details</p>
<p>(1.2) Commencement Date: Monday 23rd February 2015</p> <p>See Annex B for full timetable</p>
<p>(1.3) Price Payable by Authority £39,825 excluding VAT</p> <p>See Annex C for full details</p>
<p>(1.4) Completion Date: Monday 31st August 2015</p> <p>See Annex B for full timetable</p>

2 ADDITIONAL REQUIREMENTS
<p>(2.1) Supplemental Requirements in addition to Call-Off Terms and Conditions: None</p>
<p>(2.2) Variations to Call-Off Terms and Conditions N/A</p>

3. PERFORMANCE OF THE SERVICES [AND DELIVERABLES]
<p>(3.1) Key Personnel of the Provider to be involved in the Services [and deliverables]:</p> <p>See Annex D for details</p>
<p>(3.2) Performance Standards</p> <p>See Annex A for full details</p>
<p>(3.3) Location(s) at which the Services are to be provided:</p> <p>See Annex A for full details</p>

(3.4) Quality Standards

See Annex A for full details

(3.5) Contract Monitoring Arrangements

See Appendix 3 for full details

4. CONFIDENTIAL INFORMATION

(4.1) The following information shall be deemed Commercially Sensitive Information or Confidential Information:-

See Appendix 4 for full details

BY SIGNING AND RETURNING THIS ORDER FORM THE PROVIDER AGREES to enter a legally binding contract with the Authority to provide the Service specified in this Order Form together with, where completed and applicable, the mini-competition order (additional requirements) set out in section 2 of this Order Form. Incorporating the rights and obligations in the Call-Off Terms and Conditions set out in the Framework Agreement entered into by the Provider and UK SBS on 24/02/2014 and any subsequent signed variations to the terms and conditions.

For and on behalf of the Provider:-

Name and Title	Redacted Text
Signature	Redacted Text
Date	03/03/2015

For and on behalf of the Authority-

Name and Title	Redacted Text
Signature	Redacted Text
Date	06/03/2015

SECTION 2

APPENDIX 1 – THE SERVICES

1 General

1.1 The following additional documents shall be deemed to be incorporated into this Contract (as appropriate);

Document	Dated
Framework Call-off Terms and Conditions	24/02/2014
Specification	
Providers Tender/Proposal	

This Framework Agreement is dated 14/04/2014 OJEU reference number [2013/S 147-255782]

3 Appendices

3.1 The following annexes form part of this appendix;

- Annex A – Specification of Service Required under this Contract
- Annex B – Timetable
- Annex C – Prices, Rates and Payment Schedule
- Annex D – Provider and Sub-contractor Key Staff
- Annex E – Approved Sub-contractors

ANNEX A - Specification of Service Required under this Contract

The study universe

Whilst early phases of the (then) PNB Data Collection exercise adopted a sample-based method for collecting earnings data, in 2009-10, 2010-11, 2011-12 and 2012-13 this was replaced by a census-based approach. By moving to a census-based methodology, this not only enhanced the robustness with which data and findings could be reported, but it also facilitated earnings analysis at a far more granular level.

The 2013-14 exercise will once again adopt a census-based approach, covering all 44 Police Forces across the England, Wales and Northern Ireland, and the c. 145,000 police Officers working within them.

All Officers will be within the scope of the study, with the only exceptions being:

- Cadets and Community Support Officers; and
- Officers not in post at 31 March 2014.

Liaising with Police Forces

It is imperative that the full co-operation of Police Forces is secured and that they are involved and engaged with the survey from the outset. It is also critical that this process is made as straightforward and painless for them as possible.

It is a process we are very familiar with, and one that that relies on detailed planning, a knowledgeable and friendly Police Force liaison team, careful auditing and gritty persistence and determination.

One critical part of the process is identifying the most appropriate person to liaise with at each Police Force. Our starting point will be the list of Police Force contacts with whom we liaised for the 2012-13 exercise. There will clearly be some cases, however, where this individual is no longer the most appropriate contact (for example if they have left), and in such instances we will seek to identify the most suitable "replacement".

It should be noted that, in a previous exercise, two Police Forces had indicated that their payroll was undertaken by another force (Northamptonshire had a multi-service agreement covering Cheshire's payroll, and Leicestershire had a similar agreement covering Derbyshire's payroll). We will establish at the earliest opportunity whether such multi-service agreements are in place between any of the Forces. Similarly, there have been cases where a Force's payroll has been outsourced entirely (for example to a local Council); again, we will seek to establish any such instances at the outset and will factor this in accordingly (for example by seeing whether we can liaise with the payroll provider directly).

We would suggest that an email be sent from the Home Office to Chief Constables / Commissioners, letting them know that the exercise is about to re-commence and giving them the opportunity to nominate a different key contact point to the one on your records should they feel it appropriate. IFF would be happy to assist in the writing and expedition of these e-mails.

Once we have an up-to-date list of Police Force contacts we would begin the liaison process, the stages of which are discussed in detail below.

Introductory e-mail

Subsequent to the courtesy e-mail to Chief Constables / Commissioners, we will send an introductory e-mail to all Police Force contacts, reminding them that the exercise is taking place and of the key aims/background, and re-introducing IFF as the contractor responsible for collating the data.

This e-mail would also let them know to expect full guidance notes to be distributed around a week or so later, would give them the opportunity (again) to nominate an alternative contact if appropriate, and would invite Police Forces to reply or call in with any specific concerns that they had.

Finally, this initial e-mail will include a statement reassuring Police Forces that the pay and related data they provide will not contravene the Data Protection Act, and that confidentiality of data will be protected (i.e. that no statistics will be produced that would permit the identification of individual Officers, unless this is specifically agreed with the Officers in question).

Detailed instructions

Redacted Text

Telephone 'follow-up'

Redacted Text

Contact log

Redacted Text

Compiling the dataset

This section of the proposal details our proposed approach for compiling and collating the data collected into a complete and documented dataset.

Data validation and cleaning

Data entry

Redacted Text

Data import and cleaning

Redacted Text

Data format and the data specification

Redacted Text.

Technical and project reports

Redacted Text.

Capacity and resources

Redacted Text.

The table below highlights the key responsibilities of each member of the project team.

Team Member	Key Responsibilities
<p>Redacted Text Director</p>	<p>Overall responsibility for project and appointed Contract Manager Client contact on issues relating to design of project or in connection with any problems encountered Attendance at Steering Group meetings Design / refinement of data spreadsheets and guidance notes Sign-off of data output requirements Lead author of technical report and project report</p>
<p>Redacted Text Senior Research Executive</p>	<p>Attending Steering Group meetings Input into design / refinement of data spreadsheet and guidance notes Management of liaison with Police Forces Checking of returned data spreadsheets Provision of progress updates to the Home Office Review and input into data specification Sign-off of data outputs Input into technical report and project report</p>
<p>Redacted Text Research Executive</p>	<p>Checking and monitoring of data collection progress Checking data outputs Assisting Redacted Text with liaison with Police Forces</p>
<p>Redacted Text, Data Services Manager</p>	<p>Production of data map and input into data specification Implementation of data cleaning and validation processes Production of test data and liaison with the Home Office data team Production of final SPSS dataset and Excel tables</p>

There will be ongoing communications and feedback during the life of the studies. For example, we will liaise closely with the Home Office team to finalise all research tools, as well as to ensure that the data outputs will meet all requirements, and that the technical / project report covers all the required areas in the required depth.

Much of this will be informal by way of phone (including conference calls) and email. But it is possible that unforeseen meetings will be required. Our approach to project management is to be responsive, punctual and flexible in our dealings with you, as our client, at all times. Our size and structure as an organisation mean that while big enough to resource the largest of projects (such as this one) we are also small enough to be able to be flexible in reacting to changes or challenges as they arise.

We will also provide regular feedback on progress (at least once a week), with feedback protocols to be agreed on commissioning. As a minimum, these will include current response rates, details of progress made in chasing non-respondents (including anticipated dates for data delivery), and updates on the completeness of data supplied / proportion of responses passing the validation tests.

Data validation and cleaning

Data entry

Redacted Text

Data import and cleaning

Redacted Text.

- Data format and the data specification

Redacted Text.

- Data security and data handling

Redacted Text.

Managing the PNB pay data collection exercise

Data transfer

Redacted Text.

ANNEX B – Timetable

Week commencing	Key milestone events	Development of data spreadsheet and accompanying documents	Contact with Police Forces	Data preparation
23 rd February 2015	Contract commissioning			
9 th March	Inception meeting			
16 th March	Delivery of inception report Advance letters/emails sent by the Home Office to Chief Constables / Commissioners			
23 rd March	Introductory emails sent to Police Force contacts Finalisation of data spreadsheets and guidance notes			
30 th March	Data spreadsheets and detailed guidance notes issued to Police Forces			
6 th April	Follow-up calls to Police Forces to check receipt of 'packs' / answer initial queries			
13 th April				
20 th April				
27 th April	Initial deadline for returning data spreadsheets			
4 th May	Meeting with the Home Office analysis teams to discuss data content and format requirements			
11 th May	2 nd deadline for returning data spreadsheets Delivery of draft data specification			
18 th May				
25 th May	Finalisation of data specification			
1 st June				

OFFICIAL

8th June	Absolute deadline for returning data spreadsheets			
15th June	All queries on databases resolved as far as possible with Police Forces			
22nd June	Data cleaning			
29th June				
6th July				
13th July				
20th July				
27th July	Delivery of fully verified SPSS dataset			
3rd August	Technical and project reports delivered			
10th August	Excel data tables and Excel summary tool delivered			
17th August	Project de-briefing meeting			

ANNEX C – Prices, Rates And Payment Schedule

Resource Summary

Resource description	Rate £	Quantity / Days	*Sub Total £	*Other Costs (e.g. expenses) £	Total £ (excl. VAT)
Director Redacted Text	Redacted Text	Redacted Text			Redacted Text
Senior Research Executive Redacted Text	Redacted Text	Redacted Text			Redacted Text
Research Executive Redacted Text	Redacted Text	Redacted Text			Redacted Text
Data Services Manager Redacted Text	Redacted Text	Redacted Text			Redacted Text
Sub total					£39,575
Other Costs					
Travel and Subsistence					£250
Total					£39,825

Payment Schedule

Milestone date	Detail	Payment (£)
30 th March 2015	Inception meeting, delivery of inception report; communications sent to Chief Constables/Commissioners; introductory emails sent to Police force contacts; finalisation and issue of data spreadsheets and guidance notes to forces.	Redacted Text
25 th May 2015	Following up calls to forces completed; 1 st and 2 nd deadline for returning data spreadsheets; Meeting with HO analysis teams to discuss data content and format requirements; finalisation of data specification.	Redacted Text
27 th July 2015	Final deadline for return of all data spreadsheets; all force queries on databases resolved as far as possible; data cleaning and delivery of fully verified SPSS dataset.	Redacted Text
17 th August 2015	Technical and project reports delivered; excel data tables and excel summary tool delivered; project de-briefing meeting.	Redacted Text
Total (excluding VAT)		£39,825

Annex D – Provider and Sub-contractor Key Staff

Name	Position Held	Period of involvement in the Contract*
Redacted Text	Director	23/02/2015 – 31/08/2015
Redacted Text	Senior Research Executive	23/02/2015 – 31/08/2015
Redacted Text	Research Executive	23/02/2015 – 31/08/2015
Redacted Text	Data Services Manager	23/02/2015 – 31/08/2015

Annex E – Approved Sub-contractors

Name of Sub Contractor	Nature of the Services being Sub Contracted	Anticipated Value £

APPENDIX 2 – ADMINISTRATION REQUIREMENTS

1 Authority's Authorisation

- 1.1 The following person is the Authority's Representative and is authorised to act on behalf of the Home Office on all matters relating to the Contract, contact details are shown in the Schedule 4 (Order Form) of the Framework Agreement.

Name: Redacted Text

Title: Head of Police Employee Relations

- 1.2 The Authority's Representative may approve deputy Authority's Representatives to exercise on her behalf such powers as are contained in this Contract. The following person is authorised to act on behalf of the Home Office on all matters relating to this Contract as a Deputy Authority Representative.

Name: Redacted Text

Title: Policy Advisor, Police Employee Relations

2 Provider's Authorisation

- 2.1 The following person is the Provider's Representative and is authorised to act on behalf of the Provider on all matters relating to the Contract, contact details are shown in Schedule the (Order Form) of the Framework Agreement.

Name: Redacted Text

Title:

- 2.2 The following person is the Provider's Contract Manager and is authorised to act on behalf of the Provider on all matters relating to the Contract;

Name: Redacted Text

Title:

3 Payment Information

- 3.1 The Authority shall issue a purchase order to the Provider prior to commencement of the Service.

- 3.2 All invoices payable in compliance with the requirements of clause C2 of the call-off terms and conditions, must include the appropriate purchase order number and shall be sent to the following address;

Home Office Shared Service Centre
HO Box 5015
Newport
South Wales
NP20 9BB
Post-Room-Rescan@homeoffice.gsi.gov.uk

Shared Services Helpline: Redacted Text

- 3.3 Any additional information required independently of the invoice will be detailed in the Order Form at Call-off stage.

APPENDIX 3 – MONITORING REQUIREMENTS

This Appendix sets out the contract management requirements which are applicable to the delivery of the Services.

1 Reviewing Contract Performance

- 1.1 The Provider shall work with the Authority to establish and maintain an effective and beneficial working relationship to ensure the Contract is delivered to at least the minimum required standard as specified in the Appendix (The Services).
- 1.2 The Provider shall work with the Authority to establish suitable administrative arrangements for the effective management and performance monitoring of the Contract and shall provide information as requested to monitor and evaluate the success of the Contract and the Provider's management and delivery of it.
- 1.3 The Provider shall supply information requested relevant to the delivery of the Services to the Authority, using formats and to timescales specified by the Authority in Appendix 1, annex D.
- 1.4 The Authority intends, wherever it can, to capture and collate information through its IT system(s). However, the Authority does reserve the right to make reasonable requests for information (at no additional charge) from the Provider including ad-hoc requests for information from time to time.
- 1.5 Any additional requests for information shall be considered in consultation with the Provider as shall the process of defining the methods of collection.
- 1.6 Where an on-going, short-term or one-off requirement is agreed, both Parties agree that it shall be included, or deemed to be included within this Appendix.
- 1.7 Review meetings between the Authority and the Provider shall also cover, as appropriate, resolving disputes and/or dealing with contractual breaches in accordance with the terms and conditions of this Contract. Roles and responsibilities will be documented and the personnel involved in managing the relationship identified and suitably empowered.
- 1.8 The Authority may undertake spot checks at any time to ensure that the Provider is complying with its obligations under this Contract and the Provider shall co-operate fully, at its own cost, with the Authority.
- 1.9 The Provider will be responsible for managing and reporting on any sub-contractual arrangements. Arrangements shall include mechanisms for the provision of management information, including feedback to and from customers, stakeholders, change control procedures and the prompt resolution of any problems. The Authority will agree with the Provider day-to-day relationship management, contact points, communication flows and escalation procedures.
- 1.10 The Provider will be expected to continuously improve the quality of the provision including that delivered by Sub-contractors. Where quality falls below acceptable levels the Provider will be expected to have suitable escalation procedures in place and, in respect of sub-contracted provision, take action where necessary to terminate the contract.

2 Access

- 2.1 In all instances, the Provider shall co-operate and provide such reasonable assistance as may be necessary to facilitate such monitoring. Failure to provide such reasonable assistance shall be deemed a "Serious Breach" for the purposes of clause H2 (Termination on Default).

4 Diversity and Equality

- 4.1 The Authority will review the Provider's Diversity and Equality Delivery Plan and completed workforce monitoring data template when submitted in accordance with the Appendix (Diversity and Equality Requirements) and then annually thereafter. The Authority can request full policy/procedure documents at any time throughout the Contract.

6 Security Requirements

6.1 The Authority will review the Provider's Security Plan when submitted by the Provider in accordance with the Appendix (Security Requirements and Plan) and at least annually thereafter.

8 Health and Safety Responsibilities of the Authority Visiting Officers

8.1 The Authority representatives visit Providers and its Sub-contractors for a variety of reasons. In the course of their normal duties such representatives of the Authority shall adopt an 'eyes and ears' approach to monitoring health and safety. In doing this the Authority representatives shall not be conducting a health and safety inspection, nor shall they be in a position to offer advice on whether something is safe or not. Instead they shall approach this from the position of any lay person. If, however, the Authority representative does notice something on which they require assurance or clarification, they shall raise this with the Provider or the Sub-contractor's representative at the location where they are visiting. In no event are the Authority representatives to be seen as offering professional advice on health and safety matters and as such, shall not be liable for any advice or comments or otherwise given to the Provider or its Sub-contractors or any omission to give such advice, comments or otherwise.

SCHEDULE 6

MANAGEMENT INFORMATION (MI) REQUIREMENTS

Management Information Required	Frequency/Date Required
Contractor Financial Assurance Declaration	Within one month of submitting annual returns and accounts for the organisation to Companies House; or within 10 months of the end of the Contractor's accounting year where Contractors are not required to submit form AR01 to Companies House.
Full and final Security Plan	Within 20 Working Days after the Commencement Date and reviewed at least annually thereafter.

Appendix A – Annual Financial Assurance Declaration

Where the Provider has more than one contract with the Authority the information and returns detailed in this section will only be required at an organisational level not contract level.

1 Financial information required on an ongoing or annual basis

- 1.1 The Provider is required to disclose material changes to the organisation that impact on the ongoing financial viability including details of the revenue replacement strategy and impact awareness on the organisation's profitability and stability where significant contracts are due to end.
- 1.2 The Provider is required to notify UK SBS immediately of proposed changes to the organisational control or group structure, proposed mergers or acquisitions or proposed changes to the Provider's financial viability.
- 1.3 The Provider is required to disclose value and details of Services performed, that was not part of this Framework Agreement, but could have reasonably been actioned as a Call-Off Contract through this Framework.
- 1.4 The Provider is required to disclose all expenses incurred, whether direct or indirect in the execution of a Call-Off Contract, and give assurance to UK SBS that the Provider is making best endeavours to ensure adherence to the UK SBS Travel and Expenses policy.

2 Annual Assurance Declaration

- 2.1 The Provider will complete and return the Annual Assurance Declaration to:

UK Shared Business Services Ltd (UK SBS)
 North Star House,
 North Star Avenue,
 Swindon,
 Wiltshire, SN2 1FF

Or e-mail to
research@uksbs.co.uk

APPENDIX 4 – COMMERCIALLY SENSITIVE INFORMATION

- 1 UK SBS acknowledges that the Provider has requested that the following information be treated as Commercially Sensitive Information;

[To be inserted at contract award stage]

Document	Page Number	Section	Condition or paragraph number	Explanation of harm which may result from disclosure and time period applicable to any sensitivity

- 2 UK SBS may consult with the Provider on any request for information, identified as Commercially Sensitive, under the FOIA.
- 3 UK SBS reserves the right to disclose any Commercially Sensitive Information held within this Framework Agreement in response to a request under the FOIA as set out at Clauses C2-2 and C6 of this Agreement.
- 4 UK SBS will automatically publish all information provided by the Provider **not** identified in this Schedule as constituting Commercially Sensitive Information provided that it satisfies the requirements of the FOIA.
- 5 UK SBS reserves the right to determine whether any information provided in this Schedule does constitute Commercially Sensitive Information prior to publication.

OFFICIAL
SCHEDULE 7

FRAMEWORK AGREEMENT VARIATION PROCEDURE

1. Introduction

- 1.1 Schedule 8 details the scope of the variations permitted and the process to be followed where UK SBS proposes a variation to the Framework Agreement.
- 1.2 UK SBS may propose a variation to the Framework Agreement under Schedule 8 only where the variation does not amount to a material change in the Framework Agreement or the Services.

2. Procedure for proposing a Variation

- 2.1 Except where paragraph 5 applies, UK SBS may propose a variation using the procedure contained in this paragraph 2.
- 2.2 In order to propose a variation, UK SBS shall serve each Services Framework Provider with a Notice of Variation.
- 2.3 The Notice of Variation shall:-
- 2.3.1 contain details of the proposed variation providing sufficient information to allow each Services Framework Provider to assess the variation and consider whether any changes to the prices set out in its Pricing Matrices are necessary; and
 - 2.3.2 require each Services Framework Provider to notify UK SBS within thirty (30) days of any proposed changes to the prices set out in its Pricing Matrices.
- 2.4 Upon receipt of the Notice of Variation, each Services Framework Provider has thirty (30) days to respond in writing with any objections to the variation.
- 2.5 Where UK SBS does not receive any written objections to the variation within the timescales detailed in paragraph 2.4, UK SBS may then serve each Services Framework Provider with a written agreement detailing the variation to be signed and returned by each Services Framework Provider within thirty (30) days of receipt.
- 2.6 Upon receipt of a signed agreement from each Services Framework Provider, UK SBS shall notify all Services Framework Providers in writing of the commencement date of the variation.

3. Objections to a Variation

- 3.1 In the event that UK SBS receives one or more written objections to a variation, UK SBS may:-
- 3.1.1 withdraw the proposed variation; or
 - 3.1.2 propose an amendment to the variation.

4. Changes to the Pricing Matrices

- 4.1 Where a Services Framework Provider can demonstrate that a variation would result in a change to the prices set out in its Pricing Matrices, UK SBS may require further evidence from the Services Framework Provider that any additional costs to the Services Framework Provider will be kept to a minimum.
- 4.2 UK SBS may require the Services Framework Provider to meet and discuss any proposed changes to the Pricing Matrices that would result from a variation.
- 4.3 Where a change to The Services Framework Provider's Pricing Matrices is agreed by UK SBS, UK SBS shall notify its acceptance of the change to the Services Framework Provider in writing.

OFFICIAL

4.4 In the event that UK SBS and the Services Framework Provider cannot agree to the changes to the Pricing Matrices, UK SBS may:-

4.4.1 withdraw the variation; or

4.4.2 propose an amendment to the variation

5. **Variations which are not permitted**

5.1 In addition to the provisions contained in paragraph 1.2, UK SBS may not propose any variation which:-

5.1.1 may prevent one or more of the Services Framework Providers from performing its obligations under the Framework Agreement; or

5.1.2 is in contravention of any Law.

OFFICIAL
SCHEDULE 9

SECURITY REQUIREMENTS AND PLAN

A condition of any call off will be that the original Security Plan (identified in the RFQ Part E Specification with Bidders Response) and also at Appendix 1 will need to be updated as necessary and resubmitted with a bid unless the decision has been taken in advance that a Generic Security Accreditation Document (GSAD) will be appropriate. Information regarding GSADs will be made available if applicable to the call off contract.

UK SBS will expect Providers to achieve compliance in this process within twenty (20) Working Days [see Security Plan Development paragraph 3.3] of being awarded to this Framework Agreement. However, the Provider should also be able to demonstrate compliance already achieved during the Call-Off phase, should they subsequently be awarded a contract.

1 Introduction

1.1 This schedule covers;

- a) Principles of security for the Provider system, derived from the Security Policy, including without limitation principles of physical and information security;
- b) The creation of the Security Plan;
- c) Audit and testing of the Security Plan;
- d) Conformance to ISO/IEC: 27002 (Information Security Code of Practice) and ISO/IEC 27001 (Information Security Requirements Specification) (Standard Specification); and
- e) Breaches of security.

2 Principles of Security

2.1 The Provider acknowledges that UK SBS places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Provider System. The Provider also acknowledges the confidentiality of UK SBS's Data.

2.2 The Provider shall be responsible for the security of the Provider System and shall at all times provide a level of security which;

- a) is in accordance with Good Industry Practice and Law;
- b) complies with the Security Policy;
- c) meets any specific security threats to the Provider System.

2.3 Without limiting paragraph 2.2, the Provider shall at all times ensure that the level of security employed in the provision of the Services is appropriate to minimise the following risks:

- a) loss of integrity of Authority Data;
- b) loss of confidentiality of Authority Data;
- c) unauthorised access to, use of, or interference with Authority Data by any person or organisation;
- d) unauthorised access to network elements and buildings;
- e) use of the Provider System or Services by any third party in order to gain unauthorised access to any computer resource or Authority Data; and
- f) loss of availability of Authority Data due to any failure or compromise of the Services.

3 Security Plan

Introduction

3.1 The Provider shall develop, implement and maintain a Security Plan to apply during the Term, which will be approved by UK SBS, tested, periodically updated and audited in accordance with this Schedule.

OFFICIAL

3.2 A draft Security Plan provided by the Provider as part of its bid is set out in Appendix 1.

Development

3.3 Within twenty (20) Working Days after the Commencement Date and in accordance with paragraphs 3.10 to 3.12 (Amendment and Revision), the Provider will prepare and deliver to UK SBS for approval the full and final Security Plan which will be based on the draft Security Plan set out in Appendix 1.

3.4 If the Security Plan is approved by UK SBS it will be adopted immediately. If the Security Plan is not approved by UK SBS the Provider shall amend it within ten (10) Working Days of a notice of non-approval from UK SBS and re-submit to UK SBS 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 fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to UK SBS. If UK SBS does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with clause 37 Dispute Resolution. No approval to be given by UK SBS pursuant to this paragraph 3.4 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 3.1 to 3.9 shall be deemed to be reasonable.

Content

3.5 The Security Plan will set out the security measures in place by the Provider in relation to the Framework Agreement and shall at all times comply with:

- a) the provisions of this Framework Agreement and this schedule (including the principles set out in paragraph 2);
- b) the provisions of Appendix 1 relating to security;
- c) ISO/IEC27002 and ISO/IEC27001;
- d) the data protection compliance guidance produced by UK SBS;

3.6 The references to standards, guidance and policies set out in paragraph 3.5 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.

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

3.8 The Security Plan will be structured in accordance with ISO/IEC27002 and ISO/IEC27001.

3.9 Where the Security Plan references any document which is not in the possession of UK SBS, a copy of the document will be made available to UK SBS upon request. The Security Plan shall be written in plain English in language which is readily comprehensible to the staff of the Provider and UK SBS engaged in the Services and shall not reference any other documents which are not either in the possession of UK SBS or otherwise specified in this schedule.

Amendment and Revision

3.10 The Security Plan will be fully reviewed and updated by the Provider annually or from time to time to reflect:

- a) emerging changes in Good Industry Practice;
- b) any new perceived or changed threats to the Provider System;
- c) a reasonable request by UK SBS;

3.11 The Provider will provide UK SBS with the results of such reviews as soon as reasonably practicable after their completion and amend the Security Plan at no additional cost to UK SBS.

3.12 Any change or amendment which the Provider proposes to make to the Security Plan as a result of an Authority request or change to the Appendix 1 or otherwise shall be subject to the Framework Agreement Variation Procedure (Schedule 8) and shall not be implemented until approved in writing by UK SBS.

4 Audit and Testing

- 4.1 The Provider 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 UK SBS.
- 4.2 UK SBS shall be entitled to send a representative to witness the conduct of the Security Tests. The Provider shall provide UK SBS with the results of such tests (in a form approved by UK SBS in advance) as soon as practicable after completion of each Security Test.
- 4.3 Where any Security Test carried out pursuant to paragraphs 4.2 above reveals any actual or potential security failure or weaknesses, the Provider shall promptly notify UK SBS of any changes to the Security Plan (and the implementation thereof) which the Provider proposes to make in order to correct such failure or weakness. Subject to UK SBS's approval in accordance with paragraph 3.12, the Provider shall implement such changes to the Security Plan in accordance with the timetable agreed with UK SBS 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 UK SBS. For the purposes of this paragraph 4, a weakness means a vulnerability in security and a potential security failure means a possible breach of the Security Plan or security requirements.

5 Breach of Security

- 5.1 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.
- 5.2 Upon becoming aware of any of the circumstances referred to in paragraph 5.1, the Provider shall;
- a) immediately take all reasonable steps necessary to;
 - i) remedy such breach against any such potential or attempted breach or threat;and
 - ii) prevent an equivalent breach in the future.

Such steps shall include any action or changes reasonably required by UK SBS. In the event that such action is taken in response to a breach that is determined by UK SBS acting reasonably not to be covered by the obligations of the Provider under this Framework, then the Provider shall be entitled to refer the matter to the Framework Agreement Variation Procedure (Schedule 8).

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