Foreign, Commonwealth & Development Office

UKaid from the British people

CALL DOWN CONTRACT

Framework Agreement with: Torchlight Group Limited

Framework Agreement for: International Multi-Disciplinary Programme (IMDP), Lot 2 Conflict and Governance.

Framework Agreement Reference: PO 8373

ECM Number: ECM_5338

Call-down Contract For: South Africa: Tackling Corruption (SATaC) Programme: Provision Of Training And Capacity Development For Law Enforcement Agencies In South Africa

I refer to the following:

1. The above mentioned Framework Agreement dated 01/05/2019
2. Your proposal of 15/05/2023

and I confirm that FCDO requires you to provide the Services (Annex A), under the Terms and Conditions of the Framework Agreement which shall apply to this Call-down Contract as if expressly incorporated herein.

1. Commencement and Duration of the Services

1.1 The Supplier shall start the Services no later than **18/07/2023** ("the Start Date") and the Services shall be completed by 31/03/2025 ("the End Date") unless the Call-down Contract is terminated earlier in accordance with the Terms and Conditions of the Framework Agreement. 16.

1.2 FCDO may scale up or extend the Contract budget and/or timeframe by up to two months and £50,000 if additional law enforcement personnel require training.

2. Recipient

2.1 FCDO requires the Supplier to provide the Services to the FCDO (the "Recipient").

3. Financial Limit

3.1 Payments under this Call Down Contract shall not, exceed £385,722 ("the Financial Limit") and is exclusive of any government tax, if applicable as detailed in Annex B. When Payments shall be made on a 'Milestone Payment Basis' the following Clause 22.3 shall be substituted for Clause 22.3 of the Section 2, Framework Agreement Terms and Conditions.

22. Payments & Invoicing Instructions

22.3 Where the applicable payment mechanism is "Milestone Payment", invoices shall be submitted for the amount indicated in Annex B and payments will be made on satisfactory performance of the services, at the payment points defined as per schedule of payments. At each payment point set criteria will be defined as part of the payments. Payment will be made if the criteria are met to the satisfaction of FCDO.

Foreign, Commonwealth & Development Office

UKaid from the British people

When the relevant milestone is achieved in its final form by the Supplier or following completion of the Services, as the case may be, indicating both the amount or amounts due at the time and cumulatively. Payments pursuant to clause 22.3 are subject to the satisfaction of the Project Officer in relation to the performance by the Supplier of its obligations under the Call-down Contract and to verification by the Project Officer that all prior payments made to the Supplier under this Call-down Contract were properly due.

4. FCDO Officials

4.1 The Project Officer is: **REDACTED**

4.2 The Contract Officer is: **REDACTED**

5. Key Personnel

The following of the Supplier's Personnel cannot be substituted by the Supplier without FCDO's prior written consent:

REDACTED

6. Reports

6.1 The Supplier shall submit project reports in accordance with the Terms of Reference/Scope of Work at Annex A.

7. Call Down Contract Signature

7.1 If the original Form of Call-down Contract is not returned to the Contract Officer (as identified at clause 4 above) duly completed, signed and dated on behalf of the Supplier within 15 Working Days of the date of signature on behalf of FCDO, FCDO will be entitled, at its sole discretion, to declare this Call Down Contract void.

No payment will be made to the Supplier under this Call Down Contract until a copy of the Call Down Contract, signed on behalf of the Supplier, returned to the FCDO Contract Officer.

Foreign, Commonwealth & Development Office

Annex A

TERMS OF REFERENCE

ITT_5563 South Africa: Tackling Corruption (SATaC):
Provision of Training and Capacity Development for Law Enforcement Agencies in South Africa

IMDP Framework Call-off
Lot 2 - Conflict and Governance

Contents

Abbreviations

Acronym	Definition
BHC	British High Commission – Pretoria
CPS	Crown Prosecution Service
DPCI	Directorate for Priority Crimes Investigations (“Hawks”)
FCDO	Foreign Commonwealth and Development Office
FIC	Financial Intelligence Centre
IFF	Illicit financial flow
NCA	National Crime Agency
NPA	National Prosecuting Authority
SA	South Africa
SATaC	South Africa: Tackling Corruption Programme
SAPS	South African Police Service
SIU	Special Investigating Unit
TOR	Terms of Reference
UK	United Kingdom

Introduction

1. The Foreign Commonwealth and Development Office (FCDO) is seeking a Supplier to create and deliver a comprehensive training programme for tackling corruption in South Africa.
2. Corruption restricts inclusive economic growth, and impedes national and global economic development. It reinforces a system where a minority can prosper from positions of power and state funds can be misappropriated. This results in weak institutions; a lack of enforcement mechanisms against perpetrators; and poor public service provision that ultimately hinders the development of most citizens. Tackling corruption is integral to promoting a sustainable global economy where businesses can compete fairly, and the benefits of economic growth can be shared across society and help bring the poorest citizens out of poverty.

3. It is against this background that the South Africa: Tackling Corruption Programme (SATaC) programme aims to provide support for effective prevention and detection measures, productive investigations, and successful prosecutions to help address the challenge of corruption.

Objective of the Contract

4. The Contract objective is to support law enforcement agencies in South Africa as they enhance their capacity to effectively investigate and prosecute corruption related cases, disrupt illicit financial flows and support asset recovery.

Recipients and Beneficiaries

5. The recipients of the services are:
   - Directorate for Priority Crimes Investigations (DPCI) in South Africa
   - The National Prosecuting Authority (NPA) in South Africa,
   - The Financial Intelligence Centre and the Special Investigating Unit in in South Africa

Scope

6. The Supplier will provide appropriately skilled personnel and systems to successfully create and deliver a training package and materials including hire of venue and arrangement of equipment and refreshments that will assist the capacity building of law enforcement agencies in South Africa. Each training package will be customized and designed in consultation with FCDO and the recipients of the services, covering the in the identified priority areas:

6.1. **Financial investigation**: case management of complex commercial criminal investigations, gathering and use of digital forensics; international best practices used by law enforcement agencies in financial investigations, locating assets, and turning intelligence into evidence, international best practices used by prosecutorial services in effective prosecution of complex financial cases including corruption and procurement fraud.

6.2. **Search and Seizure:** planning (including drafting court applications), risk assessments, securing premises and preventing destruction of evidence, search techniques, command structures and decision making, use of specialists (i.e. digital forensics, dog units), preserving the chain of custody of the evidence, documenting search results and seized material, sifting seized material, dealing with legal professional privilege, seizure of digital devices.

6.3. **Open-source intelligence corruption investigations**: effective methodologies for collecting, analysing and making decisions about data in publicly available sources which can be used in an intelligence context.

6.4. **Cybercrime and crypto-assets**: understanding crypto-assets, the manner in which criminals use it to launder the proceeds of crime as well as the tools and understanding required to detect, trace, counter and investigate criminal usage of cryptocurrencies.

6.5. **Detecting and countering illicit financial flows:** understanding IFFs and its interlinkages with corruption, investigating and gathering intelligence from offshore banking, corporations and trusts, international best practices in investigating and prosecuting financial crimes stemming from IFFs.

Contract Budget and Duration

7. The contract will run for up to 21 months starting in July 2023 and ending 31 March 2025 and is subject to review points set out in detail in paragraph 10.

8. The maximum budget available for this contract will be no more than **£500,000.00** (Five Hundred Thousand GBP) (inclusive of ALL appliable taxes). There is potential to extend the Contract by up to two additional months with a budget increase of up to £50,000. See paragraph 15 for scale up/extension options.

9. The contract consists of 3 phases:

   i) **Inception phase** – 2 months
   ii) **Implementation phase** – 17 months
   iii) **Exit phase** - from completion of implementation phase to 31 March 2025

10. Movement from one phase to the next will be dependent on FCDO's acceptance of satisfactory performance and progress against the outputs specified in the agreed workplan.

The Requirements (Key Deliverables an Outputs)

11. Inception Phase Requirements

11.1. The Supplier shall deliver the following key milestones in the inception phase of the contract:

Milestone	Description	Timing
Training Workshop Plan	Finalised plan building on draft submitted as part of the bid consisting of: • A Clear agenda • Content/ syllabus • Slides consisting of learning activities/ exercises.	6 weeks after start date
Monitoring and Evaluation Plan	Finalised plan building on draft submitted as part of bid detailing approach to using feedback in improve the delivering or the project.	6 weeks after start date

12. Implementation Phase Requirements

12.1. The training will be delivered to a total of 90 members of South African law enforcement agencies (Directorate for Priority Crime Investigation, National Prosecuting Authorities, Special Investigating Unit, Financial Intelligence Centre).The Supplier shall provide stationery packs such as writing materials, training manuals and stationery if required and any other essential training materials. The supplier will be responsible for identifying a venue for the 6 training

workshops, refreshments, and lunch. The location of the training workshops will be in Pretoria for 4 training workshops and in Cape Town for 2 training workshops.

12.2. Exit Phase Requirements

i) The supplier shall provide a final assessment report on or before 28 February 2025.

The Supplier shall deliver the following outputs in the implementation and exit phase of the contract:

Milestone	Description	Timing
Training Workshops	Delivery of 6 x 8–10-day training workshops for up to 15 people per workshop focusing on the identified priority areas mentioned in section 6, and should include detail on the following requirements: • Venue identification hire • Refreshments • Equipment available/hire Workshops will be delivered in person in various locations in South Africa.	All courses delivered by January 2025
Training Workshop Assessment & Evaluation Report	Delivery of a report providing an assessment of the training workshop to Evaluate what aspects worked well and which did not and how lessons learned will be incorporated into future training sessions. Content of the assessment and evaluation report will be determined through discussion between FCDO and South African law enforcement and prosecution authorities	4 weeks after the completion of each Training Workshop
Final Assessment Report	Supplier shall provide a final assessment report. The report will include but not be limited to: • An executive summary, background to the trainings; narrative section on the delivery of the workshops, monitoring and evaluation for the whole trainings. • Recommendations to support capacity building of the law enforcement agencies divided into short, medium and long term post trainings. • Annexures that include workshop documents such as timetables, participants lists and the training workbook. Page Limit: 50 (single sided) Font: Arial 12	Exit phase, On or Before the 31 March 2025

Team Composition:

13. This project calls for a team responsible for the day-to-day management and finances of the project and with experience and capability to create and deliver the training courses.

13.1. Team of Specialists: The team of specialists will develop and deliver the training courses and will possess the following skills/expertise:

- Working knowledge of the security sector
- Areas of corruption, investigations, and prosecution
- Digital and financials forensics
- Tools and mechanisms to locate, seize and safely secure the return of illicit proceeds.
- Experience of working in Africa/South Africa or similar contexts on these issues

14. The Supplier must ensure all staff that visit South Africa are SAFE trained, as this is a requirement for official visitors.

Contract Management

Review Points

15. The contract will be subject to a review point after 12 months or 2 training workshops (whichever comes first). Continuation of the services after this point will be based on satisfactory performance delivery to that point by the supplier or satisfactory progression thereof if the delivery date of an output falls after the 12-month point.

Scale Up/Extension

16. FCDO may scale up or extend the Contract budget and/or timeframe by up to two months and £50,000 if additional law enforcement personnel require training.

Scale Down

17. FCDO reserves the right to scale down or terminate this contract in line with the Terms and Conditions. Scaling down is at FCDO's discretion and my occur for various reasons including but not limited to a change in the security situation in South Africa or shortage of funds.

Payment by Results

18. Inception Phase: Payment will be made at the end of the inception phase on completion and acceptance by FCDO of the milestones set out in paragraph 10 and in Annex B Schedule of Payments.

18.1 Implementation Phase: Payment will be made quarterly based on the completion and acceptance by FCDO of the milestones set out in paragraph 11 and Annex B Schedule of Payments,.

18.2 Exit Phase: Last payment will be after receiving the final report.

Governance

19. This section outlines how FCDO's contract with the supplier will be administered and executed over the lifecycle of SATaC training contract:

Meeting types	Occurrence	Composition	Mandates
Client meeting	Inception phase of the project	Programme Manager, NCA, CPS, supplier's representative, DPCI representative, NPA representative	Operational
Client meeting	Before each training session	Programme Manager, NCA, CPS, supplier's representative, DPCI representative, NPA representative	Operational
FCDO team meeting	After each training and reception of report	Programme Manager, NCA, CPS	Advisory
Review meeting	After 2 trainings session	Programme Manager, NCA, CPS, supplier's representative,	Approval
Final Review meeting	Exit phase – after final training	Programme Manager, NCA, CPS, DPCI representative, NPA representative	Approval

FCDO Co-ordination

19.1 The main contact for the project will be the FCDO Programme Manager based in the British High Commission in Pretoria

19.2 The main contact for Contract or commercial issues will be the Commercial Directorate Contract Officer named in the Contract.

Conflict of Interest and Gender Sensitivity

20. All outputs must be sensitive to the conflict environment and gender sensitivity, applying at a minimum the principle of 'do no harm'. The UK sees gender equality and women's rights as central to promoting peace and stability overseas. This project will take into account any gender-related differences; consider its contribution to reducing inequality between persons of different gender; and ensure that the project does no harm to any particular gender group. Gender must be fully integrated across all aspects of the intervention.

21. Gender expertise must be included across all aspects of the project: in context analysis, understanding, insight, formulation of activity objectives, identification and segmentation of target beneficiaries, strategy, design, delivery, dissemination and amplification, project staffing, methodology, monitoring and evaluation.

22. Delivered activities should cover both male and female participants and outputs must ensure they are suited to both and take into account the drivers and factors unique to both. In the assessment and evaluation reports, all data must be disaggregated (ideally by age as well as gender), with the impact of planned activity also disaggregated by men and women. If the project undertakes surveys, interviews or beneficiary analysis, the data must be gender disaggregated.

Duty of Care

23. The supplier is responsible for the safety and well-being of their personnel, supply chain members and third parties affected by their activities under this Contract. They will also be responsible for the provision of suitable security arrangements for their domestic and business property.

24. Suppliers should be familiar with the Duty of Care obligations stated within the Framework Agreement Terms and Conditions.

25. The supplier is responsible for ensuring appropriate safety and security briefings for all their personnel working under the Contract including supply chain members. Travel advice is available on the FCDO website and the Supplier must ensure they (and their personnel) and supply chain members are up to date with the latest positions.

26. Bidders must develop their proposal on the basis of being fully responsible for Duty of Care in line with the details provided above and the initial risk assessment matrix developed by FCDO (below). Bidders must confirm in the Tender that:
    - They fully accept responsibility for Security and Duty of Care.
    - They understand the potential risks and have the knowledge and experience to develop an effective risk plan.
    - They have the capability to manage their Duty of Care responsibilities throughout the life of the contract

27. If a bidder is unwilling or unable to accept responsibility for Security and Duty of Care as detailed above, their Tender will be viewed as non-compliant and excluded from further evaluation.

28. FCDO risk assessment based on location: South Africa

	South Africa
OVERALL RATING	4
FCDO travel advice	1
Host nation travel advice	Not available
Transportation	1
Security	4
Civil unrest	4
Violence/crime	4
Terrorism	3
Espionage	Not available
War	1
Hurricane	1
Earthquake	1
Floods	3
Medical Services	1

1 Very Low risk	2 Low risk	3 Med risk	**4** **High risk**	5 Very High risk
			SIGNIFICANTLY GREATER THAN NORMAL RISK	

Safeguarding

29. FCDO's approach across all its programming is to 'do no harm' by ensuring that its interventions do not sustain unequal power relations, reinforce social exclusion and predatory institutions, exacerbate conflict, contribute to human rights risks, and/or create or exacerbate resource scarcity, climate change and/or environmental damage, and/or increasing communities' vulnerabilities to shocks and trends. FCDO seeks to ensure interventions do not displace/undermine local capacity or impose long-term financial burdens on partner governments, therefore, require partners to lead and robustly consider environmental and social safeguards through their own processes with a view to meet FCDO's high standards in safeguarding and protection.

Transparency

30. FCDO requires Supplier(s) receiving and managing funds, to release open data on how this money is spent, in a common, standard, re-usable format and to require this level of information from immediate subcontractors, sub-agencies and partners.

31. It is a contractual requirement for all Supplier(s) to comply with this, and to ensure they have the appropriate tools to enable routine financial reporting, publishing of accurate data and providing evidence of this FCDO. Further information is available from: http://www.aidtransparency.net/

32. In accordance with clause 28.1 of Section 2 of Terms and Conditions, Suppliers shall publish information data to the IATI standard, that relates to a specific activity in a single, common, electronic format for the transparent, accurate, and timely comprehensive publishing of data, on all activities in the delivery chain, in the delivery of development cooperation and humanitarian aid.

UK Aid Branding

33. Suppliers who receive funding from FCDO are not required to use UK aid logo on their development and humanitarian programmes due to aid sensitivity. More information is provided on the IMDP Framework Terms and Conditions

Data protection

34. See Appendix A below.

Appendix 1 of Call-down Contract (Terms of Reference)

Schedule of Processing, Personal Data and Data Subjects

This schedule must be completed by the Parties in collaboration with each-other before the processing of Personal Data under the Contract.

The completed schedule must be agreed formally as part of the contract with FCDO and any changes to the content of this schedule must be agreed formally with FCDO under a Contract Variation.

Description	Details
Identity of the Controller and Processor for each Category of Data Subject	The Parties acknowledge that for the purposes of the Data Protection Legislation, the following status will apply to personal data under this Call-down Contract: **FCDO is the Controller and the Supplier is the Processor** in accordance with Clause 33 (Section 2 of the contract) of the following Personal Data: • personal identifiers (name, date of birth, age, gender, employment details, telephone numbers), • online identifiers (images, email addresses), • biometric data, • economic and financial data, • ID documents.
Subject matter of the processing	The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the selected law enforcement agencies and prosecuting authorities.
Duration of the processing	April 2023 – February 2025
Nature and purposes of the processing	The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction and erasure or destruction of data (whether or not by automated means). The purpose of the processing is to utilise the data to design more contextual training deliverables.
Type of Personal Data [and Special Categories of Personal Data]	The types of personal data include personal identifiers (name, date of birth, age, gender, employment details, telephone numbers), online identifiers (images, email addresses), biometric data, economic and financial data and ID documents.
Plan for return and destruction of the data once processing complete	**(UNLESS requirement under EU or European member state law to preserve that type of data)**

Foreign, Commonwealth & Development Office

Appendix 2 of Call-down Contract (Terms of Reference)

Joint Control: Data Sharing Agreement

1.1 With respect to Personal Data which has been identified in Appendix 1 as under Joint Control of the Parties because envisage that they shall jointly determine the purpose and means of processing and each be a Data Controller in respect of that Personal Data. Accordingly, the Parties each undertake to comply with the applicable Data Protection Law in respect of their Processing of such Personal Data as Joint Data Controllers.

1.2 The Supplier shall be the exclusive point of contact for Data Subjects in Appendix 1 In who shall:

(a) direct Data Subjects to the exclusive point of contact's Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(b) be responsible for the Parties' compliance with all duties to provide information under Articles 13 and 14 of the GDPR; and

(c) shall make available to Data Subjects the essence of this Clause Data Sharing Agreement (and notify them of any changes to it) concerning allocation of responsibilities as Joint Controller and its role as exclusive point of contact. This must be outlined in the exclusive point of contact's privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 The Joint Controllers each undertake that they shall:

(a) report to the other Party every three months on:

(i) the volume of Data Subject Access Requests (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Law;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;

that it has received in relation to the Personal Data under Joint Control during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 1.3(a) (i) to (v); and

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 1.3(a) (iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Law.

(d) obtain the consent of Data Subjects or carrying out and documenting legitimate interest assessments, in accordance with the GDPR, for all Processing;

(e) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, save where such disclosure or transfer is specifically authorised under this Agreement or is required by Law). For the avoidance of doubt to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex.

(f) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information.

(g) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data

(h) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Appendix 2 (*Data Sharing Agreement*) and those in respect of Confidential Information

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where that Party would not be permitted to do so;

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Law;

(i) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures.

(j) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Law, to provide or correct or delete at

the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

(i) ensure that it notifies the other Party promptly and in any event within 48 hours if it becomes aware of a Data Loss Event.

1.4 Each Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Law and shall not perform its obligations under this Appendix in such a way as to cause the other Controller to breach any of the / its obligations under applicable Data Protection Law to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

1.5 Each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(i) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Laws;

(ii) all reasonable assistance, including:

(a) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(b) co-operation with the other Party including taking such reasonable steps as are requested by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(c) reasonable co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach;

(d) providing the other Party and to the extent requested by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 1.6.

.

1.6 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as if it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours upon becoming aware of the Personal Data Breach relating to the Personal Data Breach, in particular:

(i) the nature of the Personal Data Breach;

(ii) the nature of Personal Data affected;

(iii) the categories and number of Data Subjects concerned;

(iv) the name and contact details of the Provider's Data Protection Officer or other relevant contact from whom more information may be obtained;

(v) measures taken or proposed to be taken to address the Personal Data Breach; and

(vi) describe the likely consequences of the Personal Data Breach.

1.7 The Parties shall:

(a) provide all reasonable assistance to the each other in preparing any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to processing operations, risks and measures);

(b) maintain full and complete records of all processing carried out in respect of the Personal Data in connection with this [Framework Agreement/Call-down Contract], such records shall include the following information:

(i) the categories and purposes of processing carried out in respect of the Personal Data;

(ii) where applicable, complete information about transfers of Personal Data outside the EU, and the safeguards implemented in respect of such transfers necessary to comply with Law;

(iii) a general description of the Protective Measures which the Provider has implemented to safeguard the Personal Data in accordance with this clause and in compliance with Law.

1.8 If financial penalties are imposed by the Information Commissioner on either Joint Controller for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

(a) If the FCDO is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the FCDO, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the FCDO, then the FCDO shall be responsible for the payment of such Financial Penalties. In this case, the FCDO will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such data incident. The Supplier shall provide to the FCDO and its third party investigators and auditors, on request and at the FCDO's reasonable cost, full cooperation and access to conduct a thorough audit of such data incident;

(b) If the Supplier is responsible for the Personal Data Breach, in that it is not a breach that the FCDO is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The FCDO will provide to the

Supplier and its auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such data incident.

(c) If responsibility is unclear, then the Joint Controllers shall work together to investigate the relevant data incident and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to Dispute Resolution.

1.9 If any of the Joint Controllers is the defendant in a legal claim brought by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of a court of competent jurisdiction or the Information Commissioner to be responsible for the Personal Data Breach shall be liable for the losses arising from such breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court or the Information Commissioner, as the case may be.

1.10 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) the Party responsible for the relevant breach shall be responsible for the Claim Losses; and

(b) if responsibility is unclear, then the Parties shall be responsible for the Claim Losses equally.

1.11 In respect of any Processing of Personal Data under Joint Control by a sub-contractor or agents of a Party, each Party shall:

(i) carry out adequate due diligence on such third party or the sub-contractor to ensure that it is capable of providing the level of protection for the Personal Data as is required by Clause 1.3(e), and provide evidence of such due diligence to the other Party where reasonably requested by the other Party or the Information Commissioner; and

(ii) ensure that a suitable agreement is in place with the third party or the Sub-contractor or Key Sub-contractor including as may be required under applicable Data Protection Law.

1.12 The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be appropriate for them to retain such Personal Data under applicable Data Protection Law and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by this Agreement), and taking all further actions as may be necessary or desirable to ensure its compliance with Data Protection Law and its privacy policy.

Foreign, Commonwealth & Development Office

UKaid from the British people

Annex B

SCHEDULE OF PRICES

1. It is a requirement that all invoices are presented in the format of the payment basis, and in the case of Fees and Expenses only those categories defined are separately identified. Only one invoice per period, as defined in the Framework Agreement Terms and Conditions of Section 2, Clause 22, should be submitted.

2. **Milestone Payments**

The amount to be paid for the completion of the services is fixed at £385,722

Payment will be made on satisfactory performance of the services, at the payment points defined below (schedule of payments):

(i) at relevant points throughout the contract period.

At each payment point set criteria will be defined as part of the schedule of payments. Payment will be made if the criteria are met to the satisfaction of FCDO.

Schedule of Payments:

REDACTED