DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Award Form

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

This Award Form creates the Framework Contract. It summarises the main features of the procurement and includes the Buyer and the Supplier's contact details.

1.	**Buyer**	Food Standards Agency (the Buyer) Its offices are on: Clive House 70 Petty France London, SW1H 9EX
2.	**Supplier**	Name: CCL-Forensics Ltd Address: 36 Cygnet Court, Stratford-upon-Avon, Warwickshire, CV37 9NW Registration number: **05314495**registration number if registered] SID4GOV ID: SID4GOV ID if you have one]
3.	**Framework ontract**	This Framework Contract between the Buyer and the Supplier is for the supply of Deliverables. This opportunity is advertised in the Contract Notice in the Official Journal of the European Union reference 2020/S 115-280654 (OJEU Contract Notice).
4.	**Framework Reference**	FS900084
5.	**Deliverables**	See Schedule 2 (Specification) for further details.
6.	**Framework Start Date**	1st November 2020
7.	**Framework End Date**	31st October 2022
8.	**Framework Optional Extension Period**	Maximum of 2 Years
9.	**Incorporated Terms**	The following documents are incorporated into the Framework Contract. Where numbers are missing, we are not using these Schedules. If the documents conflict, the following order of precedence applies:

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

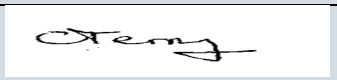
	(together these documents form the 'the Framework Contract')	• This Framework Award Form • Any Framework Special Terms (see **Section 10 Special Terms** in this Award Form) • Core Terms (version 1.0) • Schedule 1 (Definitions) • Schedule 20 (Processing Data) • The following Schedules (in equal order of precedence): • Schedule 2 (Specification) • Schedule 3 (Charges) • Schedule 4 (Tender) • Schedule 6 (Work Package Call-Off Order Procedure and Order Form) • Schedule 13 (Contract Management) • Schedule 16 (Security) • Schedule 20 (Processing Data) • Schedule 21 (Variation Form) • Schedule 22 (Insurance Requirements) • Schedule 27 (Key Subcontractors)
10.	**Special Terms**	N/A
11.	**Social Value Commitment**	The Supplier agrees, in providing the Deliverables and performing its obligations under the Framework Contract, that it will comply with the social value commitments in Schedule 4 (Tender)
12.	**Commercially Sensitive Information**	Supplier's Commercially Sensitive Will be reviewed in each work order call off Schedule 6
13.	**Charges**	Details in Schedule 3 (Charges)
14.	**Reimbursable expenses**	Recoverable as set out in Schedule 3 (Charges)
15.	**Payment Method**	All invoices must be sent, quoting a valid purchase order number (PO Number), to: Accounts-Payable.fsa@gov.sscl.com

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

		Within 10 Working Days of receipt of your countersigned copy of this letter, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice. To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, PO Number item number (if applicable) and the details (name and telephone number) of your Buyer contact (i.e. Framework Contract Manager). Non-compliant invoices will be sent back to you, which may lead to a delay in payment. If you have a query regarding an outstanding payment, please contact our Accounts Payable section either by email to [Insert email address] or by telephone [Insert telephone number] between 09:00-17:00 Monday to Friday.
16.	**Insurance**	Details in Annex of Schedule 22 (Insurance Requirements).
17.	**Liability**	In accordance with Clause 11.1 of the Core Terms each Party's total aggregate liability in each Framework Contract Year under the Framework Contract (whether in tort, contract or otherwise) is no more than [the greater of £**5 million.**
18.	**Supplier Framework Contract Manager**	Samantha Ollis Bid Manager sam.ollis@cclsolutionsgroup.com 01789 261200
19.	**Key Subcontractors**	**Key Subcontractor 1** Name (Registered name if registered) [**insert** name] Registration number (if registered) [**insert** number] Role of Subcontractor [**insert** role] **[Guidance:** copy above lines as needed]
20.	**Buyer Authorised Representative**	Andrew Quinn Deputy Head of Unit Investigations Command Andrew.Quinn@food.gov.uk +44 (0)7881 835302

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Signed for and on behalf of the **Supplier**	Signed for and on behalf of the **Buyer**
Name: **Noel mcMenamin** Chief Executive Officer	Name: Caroline Terry Commercial Business Partner
Date: 10/26/2020	Date:26/11/2020
Signature: DocuSigned by: Noel McMenamin 1C4CB5E68BEC4B6...	Signature: 

Core Terms

1. Definitions used in the Framework Contract

1.1 Interpret this Framework Contract using Schedule 1 (Definitions).

2. How the Framework Contract works

2.1 The Supplier is eligible for the award of Work package Call-Off during the Framework Contract Period.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

The Buyer doesn't guarantee the Supplier any exclusivity, quantity or value of work under the Framework Contract. The buyer has paid one penny to the Supplier legally to form the Framework Contract. The Supplier acknowledges this payment.

If the Buyer decides to buy Deliverables under the Framework Contract it must state its requirements using the Work Package Call Off Order Form). If allowed by the Regulations, the Buyer can:

- make changes to Framework Schedule 6 (Work Package Call-Off Order Form)
- create new Schedules
- exclude optional template Schedules
- use Special Terms in the Award Form to add or change terms

2.2 Each Call-Off Contract:

- is a separate Contract from the Framework Contract
- is between the Supplier and the buyer for that specific piece of work
- includes Core Terms, Schedules and any other changes or items in the completed Order Form
- survives the termination of the Framework Contract

2.3 The Supplier acknowledges it has all the information required to perform its obligations under the Framework Contract before entering into it. When information is provided by the Buyer no warranty of its accuracy is given to the Supplier.

2.4 The Supplier won't be excused from any obligation, or be entitled to additional Costs or Charges because it failed to either:

- verify the accuracy of the Due Diligence Information
- properly perform its own adequate checks

2.5 The Buyer will not be liable for errors, omissions or misrepresentation of any information.

2.6 The Supplier warrants and represents that all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

3. What needs to be delivered

3.1 All deliverables

3.1.1 The Supplier must provide Deliverables:

- that comply with the Specification, the Tender Response and the Call-off Order form

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- using Good Industry Practice
- using its own policies, processes and internal quality control measures as long as they don't conflict with the Framework Contract
- on the dates agreed
- that comply with Law

3.1.2 In the event that a level of warranty is not specified in the Award Form, the Supplier must provide Deliverables with a warranty of at least 90 days from Delivery against all obvious defects.

3.2 Goods clauses

3.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.

3.2.2 All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.

3.2.3 The Supplier transfers ownership of the Goods on Delivery or payment for those Goods, whichever is earlier.

3.2.4 Risk in the Goods transfers to the Buyer on Delivery of the Goods, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

3.2.5 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

3.2.6 The Supplier must deliver the Goods on the date and to the specified location during the Buyer's working hours.

3.2.7 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

3.2.8 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

3.2.9 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.

3.2.10 The Supplier must indemnify the Buyer against the costs of any Recall of the Goods and give notice of actual or anticipated action about the Recall of the Goods.

3.2.11 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days notice then it will pay the Supplier's

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable steps to minimise these costs.

3.2.12 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they don't conform with Clause 3. If the Supplier doesn't do this it will pay the Buyer's costs including repair or re-supply by a third party.

3.3 Services clauses

3.3.1 Late Delivery of the Services will be a Default of the Framework Contract.

3.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the Delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions of the Buyer or third party suppliers.

3.3.3 The Supplier must at its own risk and expense provide all Supplier Equipment required to Deliver the Services.

3.3.4 The Supplier must allocate sufficient resources and appropriate expertise to the Framework Contract.

3.3.5 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.

3.3.6 The Supplier must ensure all Services, and anything used to Deliver the Services, are of good quality and free from defects.

3.3.7 The Buyer is entitled to withhold payment for partially or undelivered Services but doing so does not stop it from using its other rights under the Framework Contract.

4 Pricing and payments

4.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the Charges in the Award Form.

4.2 All Charges:

- exclude VAT, which is payable on provision of a valid VAT invoice
- include all costs connected with the Supply of Deliverables

4.3 The Buyer must pay the Supplier the Charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds using the payment method and details stated in the Award Form.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

4.4 A Supplier invoice is only valid if it:

- includes all appropriate references including the Framework Contract reference number and other details reasonably requested by the Buyer
- includes a detailed breakdown of Delivered Deliverables and Milestone(s) (if any)

4.5 The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.

4.6 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this does not happen, the Buyer can publish the details of the late payment or non-payment.

4.7 If the Buyer can get more favourable commercial terms for the supply at cost of any materials, goods or services used by the Supplier to provide the Deliverables and that cost is reimbursable by the Buyer, then the Buyer may either:

- require the Supplier to replace its existing commercial terms with the more favourable terms offered for the relevant items; or
- enter into a direct agreement with the Subcontractor or third party for the relevant item

4.8 If the Buyer uses Clause 4.7 then the Charges must be reduced by an agreed amount by using the Variation Procedure.

4.9 The Buyer's right to enter into a direct agreement for the supply of the relevant items is subject to both:

- the relevant item being made available to the Supplier if required to provide the Deliverables
- any reduction in the Charges excludes any unavoidable costs that must be paid by the Supplier for the substituted item, including any licence fees or early termination charges

4.10 The Supplier has no right of set-off, counterclaim, discount or abatement unless they’re ordered to do so by a court.

5. The buyer’s obligations to the supplier

5.1 If Supplier Non-Performance arises from a Buyer Cause:

- the Buyer cannot terminate the Framework Contract under Clause 10.4.1

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- the Supplier is entitled to reasonable and proven additional expenses and to relief from Delay Payments, liability and Deduction under this Framework Contract
- the Supplier is entitled to additional time needed to make the Delivery
- the Supplier cannot suspend the ongoing supply of Deliverables

5.2 Clause 5.1 only applies if the Supplier:

- gives notice to the Buyer of the Buyer Cause within 10 Working Days of becoming aware
- demonstrates that the Supplier Non-Performance only happened because of the Buyer Cause
- mitigated the impact of the Buyer Cause

6. Record keeping and reporting

6.1 The Supplier must attend Progress Meetings with the Buyer and provide Progress Reports when specified in the Order Form.

6.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Framework Contract for 7 years after the End Date and in accordance with the GDPR.

6.3 The Supplier must allow any Auditor access to their premises to verify all Framework Contract accounts and records of everything to do with the Framework Contract and provide copies for an Audit.

6.4 The Supplier must provide information to the Auditor and reasonable co-operation at their request.

6.5 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

- tell the Buyer and give reasons
- propose corrective action

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- provide a deadline for completing the corrective action

7. Supplier staff

7.1 The Supplier Staff involved in the performance of the Framework Contract must:

- be appropriately trained and qualified
- be vetted using Good Industry Practice and the Security Policy
- comply with all conduct requirements when on the Buyer's Premises

7.2 Where the Buyer decides one of the Supplier's Staff is not suitable to work on the Framework Contract, the Supplier must replace them with a suitably qualified alternative.

7.3 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach Clause 27.

7.4 The Supplier must provide a list of Supplier Staff needing to access the Buyer's Premises and say why access is required.

7.5 The Supplier indemnifies the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8. Rights and protection

8.1 The Supplier warrants and represents that:

- it has full capacity and authority to enter into and to perform the Framework Contract
- the Framework Contract is executed by its authorised representative
- it is a legally valid and existing organisation incorporated in the place it was formed
- there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might affect its ability to perform the Framework Contract
- it maintains all necessary rights, authorisations, licences and consents to perform its obligations under the Framework Contract

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform the Framework Contract
- it is not impacted by an Insolvency Event
- it will comply with each Call-Off

8.2 The warranties and representations in Clauses 2.6 and 8.1 are repeated each time the Supplier provides Deliverables under the Framework Contract.

8.3 The Supplier indemnifies the Buyer against each of the following:

- wilful misconduct of the Supplier, Subcontractor and Supplier Staff that impacts the Framework Contract
- non-payment by the Supplier of any tax or National Insurance

8.4 All claims indemnified under this Framework Contract must use Clause 26.

8.5 The Buyer can terminate the Framework Contract for breach of any warranty or indemnity where they are entitled to do so.

8.6 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify the Buyer.

8.7 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier.

9. Intellectual Property Rights (IPRs)

9.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable it to both:

- receive and use the Deliverables
- make use of the deliverables provided by a Replacement Supplier

9.2 Any New IPR created under the Framework Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs and New IPRs for the purpose of fulfilling its obligations during the Framework Contract Period.

9.3 Where a Party acquires ownership of IPRs incorrectly under this Framework Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

9.4 Neither Party has the right to use the other Party's IPRs, including any use of the other Party's names, logos or trademarks, except as provided in Clause 9 or otherwise agreed in writing.

9.5 If there is an IPR Claim, the Supplier indemnifies the Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.

9.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:

- obtain for the Buyer the rights in Clause 9.1 and 9.2 without infringing any third party IPR
- replace or modify the relevant item with substitutes that don't infringe IPR without adversely affecting the functionality or performance of the Deliverables

10. Ending the Framework Contract

10.1 The Framework Contract takes effect on the Start Date and ends on the End Date or earlier if required by Law.

10.2 The Buyer can extend the Framework Contract for the Extension Period by giving the Supplier no less than 3 Months' written notice before the Framework Contract expires.

10.3 Ending the Framework Contract without a reason

10.3.1 The Buyer has the right to terminate the Framework Contract at any time without reason or liability by giving the Supplier at least 90 days' notice and if it's terminated Clause 10.5.2 to 10.5.7 applies.

10.4 When the Buyer can end the Framework Contract

10.4.1 If any of the following events happen, the Buyer has the right to immediately terminate the Framework Contract by issuing a Termination Notice to the Supplier:

- there's a Supplier Insolvency Event
- there's a Default that is not corrected in line with an accepted Rectification Plan
- the Buyer rejects a Rectification Plan or the Supplier does not provide it within 10 days of the request

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- there's any material Default of the Framework Contract
- there's any material Default of any Joint Controller Agreement relating to the Framework Contract
- there's a Default of Clauses 2.6, 9, 14, 15, 27, 32 or Schedule 19 (Cyber Essentials) (where applicable) relating to the Framework Contract
- there's a consistent repeated failure to meet the Service Levels in Schedule 10 (Service Levels)
- there's a Change of Control of the Supplier which isn't pre-approved by the Buyer in writing
- there's a Variation to the Framework Contract which cannot be agreed using Clause 24 (Changing the Framework Contract) or resolved using Clause 34 (Resolving disputes)
- The Buyer discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Framework Contract was awarded
- the Court of Justice of the European Union uses Article 258 of the Treaty on the Functioning of the European Union (TFEU) to declare that the Framework Contract should not have been awarded to the Supplier because of a serious breach of the TFEU or the Regulations
- the Supplier or its Affiliates embarrass or bring the Buyer into disrepute or diminish the public trust in them

10.4.2 If there is a Default, the Buyer can, without limiting its other rights, request that the Supplier provide a Rectification Plan.

10.4.3 When the Buyer receives a requested Rectification Plan it can either:

- reject the Rectification Plan or revised Rectification Plan, giving reasons
- accept the Rectification Plan or revised Rectification Plan (without limiting its rights) and the Supplier must immediately start work on the actions in the Rectification Plan at its own cost, unless agreed otherwise by the Parties

10.4.4 Where the Rectification Plan or revised Rectification Plan is rejected, the Buyer:

- must give reasonable grounds for its decision
- may request that the Supplier provides a revised Rectification Plan within 5 Working Days

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

10.4.5 If any of the events in 73 (1) (a) to (c) of the Regulations happen, the Buyer has the right to immediately terminate the Framework Contract and Clause 10.5.2 to 10.5.7 applies.

10.5 What happens if the Framework Contract ends

Where the Buyer terminates the Framework Contract under Clause 10.4.1 all of the following apply:

10.5.1 The Supplier is responsible for the Buyer's reasonable costs of procuring Replacement Deliverables for the remainder of any outstanding Work Package Call off's.

10.5.2 The Buyer's payment obligations under the terminated Framework Contract stop immediately.

10.5.3 Accumulated rights of the Parties are not affected.

10.5.4 The Supplier must promptly delete or return the Government Data except where required to retain copies by law.

10.5.5 The Supplier must promptly return any of the Buyer's property provided under the terminated Framework Contract.

10.5.6 The Supplier must, at no cost to the Buyer, co-operate fully in the handover and re-procurement (including to a Replacement Supplier).

10.5.7 The following Clauses survive the termination of the Framework Contract: 3.2.10, 6, 7.2, 9, 11, 14, 15, 16, 17, 18, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

10.6 When the supplier can end the Framework Contract

10.6.1 The Supplier can issue a Reminder Notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate the Framework Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the total Framework Contract Value within 30 days of the date of the Reminder Notice.

10.6.2 If a Supplier terminates the Framework Contract under Clause 10.6.1:

- the Buyer must promptly pay all outstanding Charges incurred to the Supplier
- the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Framework Contract had not been terminated

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- Clauses 10.5.4 to 10.5.7 apply

10.7 When subcontracts can be ended

At the Buyer's request, the Supplier must terminate any Subcontracts in any of the following events:

- there is a Change of Control of a Subcontractor which isn't pre-approved by the Buyer in writing
- the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 10.4
- a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Buyer

10.8 Partially ending and suspending the Framework Contract

10.8.1 Where the Buyer has the right to terminate the Framework Contract it can terminate or suspend (for any period), and the Supplier cannot enter into any new Call-Off Contracts during this period. If this happens, the Supplier must still meet its obligations under any existing Call-Off Contracts that have already been signed.

10.8.1 Where the FSA has the right to terminate a Framework Contract it is entitled to terminate all or part of it.

10.8.2 Where the buyer has the right to terminate a Call-Off it can terminate or suspend (for any period), all or part of it. If the buyer suspends a Call Off it can provide the Deliverables itself or buy them from a third party.

10.8.3 The buyer can only partially terminate or suspend a call off if the remaining parts of that call off can still be used to effectively deliver the intended purpose.

10.8.3 The Parties must agree any necessary Variation required by Clause 10.8 using the Variation Procedure, but the Supplier may not either:

- reject the Variation
- increase the Charges, except where the right to partial termination is under Clause 10.3

10.8.4 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under Clause 10.8.

11. How much you can be held responsible for

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

11.1 Each Party's total aggregate liability in each Framework Contract Year under the Framework Contract (whether in tort, Framework Contract or otherwise) is no more than the greater of £5 million or 150% of the Estimated Yearly Charges unless specified in the Award Form.

11.2 No Party is liable to the other for:

- any indirect Losses
- Loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect)

11.3 In spite of Clause 11.1, neither Party limits or excludes any of the following:

- its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors
- its liability for bribery or fraud or fraudulent misrepresentation by it or its employees
- any liability that cannot be excluded or limited by Law

11.4 In spite of Clause 11.1, the Supplier does not limit or exclude its liability for any indemnity given under Clauses 7.5, 8.3, 9.5, 12.2 or 14.8 or Schedule 7 (Staff Transfer) of the Framework Contract.

11.5 Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with the Framework Contract, including any indemnities.

11.6 When calculating the Supplier's liability under Clause 11.1 the following items will not be taken into consideration:

- Deductions
- any items specified in Clause 11.4

11.7 If more than one Supplier is party to the Framework Contract, each Supplier Party is fully responsible for both their own liabilities and the liabilities of the other Suppliers.

12. Obeying the law

12.1 The Supplier must use reasonable endeavours to comply with the provisions of Schedule 26 (Corporate Social Responsibility).

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

12.2 The Supplier indemnifies the Buyer against any costs resulting from any Default by the Supplier relating to any applicable Law.

12.3 The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, Clause 12.1 and Clauses 27 to 32.

13. Insurance

The Supplier must, at its own cost, obtain and maintain the Required Insurances in Schedule 22 (Insurance Requirements).

14. Data protection

14.1 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with Schedule 20 (Processing Data).

14.2 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.3 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every 6 Months.

14.4 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the Security Policy and any applicable Security Management Plan.

14.5 If at any time the Supplier suspects or has reason to believe that the Government Data provided under the Framework Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Buyer and immediately suggest remedial action.

14.6 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Buyer may either or both:

- tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Buyer receives notice, or the Supplier finds out about the issue, whichever is earlier
- restore the Government Data itself or using a third party

14.7 The Supplier must pay each Party's reasonable costs of complying with Clause 14.6 unless the Buyer is at fault.

14.8 The Supplier:

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- must provide the Buyer with all Government Data in an agreed open format within 10 Working Days of a written request
- must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading
- must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice
- securely erase all Government Data and any copies it holds when asked to do so by the Buyer unless required by Law to retain it
- indemnifies the Buyer against any and all Losses incurred if the Supplier breaches Clause 14 and any Data Protection Legislation.

15. What you must keep confidential

15.1 Each Party must:

- keep all Confidential Information it receives confidential and secure
- not disclose, use or exploit the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent, except for the purposes anticipated under the Framework Contract
- immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information

15.2 In spite of Clause 15.1, a Party may disclose Confidential Information which it receives from the Disclosing Party in any of the following instances:

- where disclosure is required by applicable Law or by a court with the relevant jurisdiction if the Recipient Party notifies the Disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure
- if the Recipient Party already had the information without obligation of confidentiality before it was disclosed by the Disclosing Party
- if the information was given to it by a third party without obligation of confidentiality
- if the information was in the public domain at the time of the disclosure
- if the information was independently developed without access to the Disclosing Party's Confidential Information

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- to its auditors or for the purposes of regulatory requirements
- on a confidential basis, to its professional advisers on a need-to-know basis
- to the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010

15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Framework Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Buyer at its request.

15.4 The Buyer may disclose Confidential Information in any of the following cases:

- on a confidential basis to the employees, agents, consultants and contractors of the Buyer
- on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that the Buyer transfers or proposes to transfer all or any part of its business to
- if the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions
- where requested by Parliament
- under Clauses 4.7 and 16

15.5 For the purposes of Clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in Clause 15.

15.6 Transparency Information and any Information which is exempt from disclosure by Clause 16 is not Confidential Information.

15.7 The Supplier must not make any press announcement or publicise the Framework Contracts or any part of them in any way, without the prior written consent of the Buyer and must take all reasonable steps to ensure that Supplier Staff do not either.

16. When you can share information

16.1 The Supplier must tell the Buyer within 48 hours if it receives a Request For Information.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

16.2 Within the required timescales the Supplier must give the Buyer full co-operation and information needed so the Buyer can:

- publish the Transparency Information
- comply with any Freedom of Information Act (FOIA) request
- comply with any Environmental Information Regulations (EIR) request

16.3 The Buyer may talk to the Supplier to help it decide whether to publish information under Clause 16. However, the extent, content and format of the disclosure is the Buyer's decision, which does not need to be reasonable.

17. Invalid parts of the Framework Contract

If any part of the Framework Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Framework Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Framework Contract, whether it's valid or enforceable.

18. No other terms apply

The provisions incorporated into the Framework Contract are the entire agreement between the Parties. The Framework Contract replaces all previous statements and agreements whether written or oral. No other provisions apply.

19. Other people's rights in the Framework Contract

No third parties may use the Framework Contracts (Rights of Third Parties) Act (CRTPA) to enforce any term of the Framework Contract unless stated (referring to CRTPA) in the Framework Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

20. Circumstances beyond your control

20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under the Framework Contract while the inability to perform continues, if it both:

- provides a Force Majeure Notice to the other Party
- uses all reasonable measures practical to reduce the impact of the Force Majeure Event

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

20.2 Either party can partially or fully terminate the affected Framework Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

20.3 Where a Party terminates under Clause 20.2:

- each party must cover its own Losses
- Clause 10.5.2 to 10.5.7 applies

21. Relationships created by the Framework Contract

The Framework Contract does not create a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22. Giving up Framework Contract rights

A partial or full waiver or relaxation of the terms of the Framework Contract is only valid if it is stated to be a waiver in writing to the other Party.

23. Transferring responsibilities

23.1 The Supplier cannot assign the Framework Contract without the Buyer's written consent.

23.2 The Buyer can assign, novate or transfer its Framework Contract or any part of it to any Crown Body, public or private sector body which performs the functions of the Buyer.

23.3 When the Buyer uses its rights under Clause 23.2 the Supplier must enter into a novation agreement in the form that the Buyer specifies.

23.4 The Supplier can terminate the Framework Contract novated under Clause 23.2 to a private sector body that is experiencing an Insolvency Event.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

23.6 If the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:

- their name

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- the scope of their appointment
- the duration of their appointment

24. Changing the Framework Contract

24.1 Either Party can request a Variation to the Framework Contract which is only effective if agreed in writing and signed by both Parties

24.2 The Supplier must provide an Impact Assessment either:

- with the Variation Form, where the Supplier requests the Variation
- within the time limits included in a Variation Form requested by the Buyer

24.3 If the Variation to the Framework Contract cannot be agreed or resolved by the Parties, the Buyer can either:

- agree that the Framework Contract continues without the Variation
- terminate the affected Framework Contract, unless the Supplier has already provided part or all of the provision of the Deliverables, or where the Supplier can show evidence of substantial work being carried out to provide them
- refer the Dispute to be resolved using Clause 34 (Resolving Disputes)

24.4 The Buyer is not required to accept a Variation request made by the Supplier.

24.5 If there is a General Change in Law, the Supplier must bear the risk of the change and is not entitled to ask for an increase to the Charges.

24.6 If there is a Specific Change in Law or one is likely to happen during the Framework Contract Period the Supplier must give the Buyer notice of the likely effects of the changes as soon as reasonably practical. They must also say if they think any Variation is needed either to the Deliverables, the Charges or the Framework Contract and provide evidence:

- that the Supplier has kept costs as low as possible, including in Subcontractor costs
- of how it has affected the Supplier’s costs

24.7 Any change in the Charges or relief from the Supplier's obligations because of a Specific Change in Law must be implemented using Clauses 24.1 to 24.4.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

25. How to communicate about the Framework Contract

25.1 All notices under the Framework Contract must be in writing and are considered effective on the Working Day of delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective when sent unless an error message is received.

25.2 Notices to the Buyer must be sent to the Buyer Authorised Representative's address or email address in the Award Form.

25.3 This Clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

26. Dealing with claims

26.1 If a Beneficiary is notified of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days.

26.2 At the Indemnifier's cost the Beneficiary must both:

- allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim
- give the Indemnifier reasonable assistance with the claim if requested

26.3 The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which cannot be unreasonably withheld or delayed.

26.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that doesn't damage the Beneficiary's reputation.

26.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

26.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.

26.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers money which is directly related to the Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:

- the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money
- the amount the Indemnifier paid the Beneficiary for the Claim

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

27. Preventing fraud, bribery and corruption

27.1 The Supplier must not during any Framework Contract Period:

- commit a Prohibited Act or any other criminal offence in the Regulations 57(1) and 57(2)
- do or allow anything which would cause the Buyer, including any of their employees, consultants, contractors, Subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them

27.2 The Supplier must during the Framework Contract Period:

- create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its Subcontractors to do the same
- keep full records to show it has complied with its obligations under Clause 27 and give copies to the Buyer on request
- if required by the Buyer, within 20 Working Days of the Start Date of the Framework Contract, and then annually, certify in writing to the Buyer, that they have complied with Clause 27, including compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures

27.3 The Supplier must immediately notify the Buyer if it becomes aware of any breach of Clauses 27.1 or 27.2 or has any reason to think that it, or any of the Supplier Staff, has either:

- been investigated or prosecuted for an alleged Prohibited Act
- been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any government department or agency
- received a request or demand for any undue financial or other advantage of any kind related to the Framework Contract
- suspected that any person or Party directly or indirectly related to the Framework Contract has committed or attempted to commit a Prohibited Act

27.4 If the Supplier notifies the Buyer as required by Clause 27.3, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

27.5 In any notice the Supplier gives under Clause 27.4 it must specify the:

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- Prohibited Act
- identity of the Party who it thinks has committed the Prohibited Act
- action it has decided to take

28. Equality, diversity and human rights

28.1 The Supplier must follow all applicable equality Law when they perform their obligations under the Framework Contract, including:

- protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise
- any other requirements and instructions which the Buyer reasonably imposes related to equality Law

28.2 The Supplier must take all necessary steps, and inform the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on the Framework Contract.

29. Health and safety

29.1 The Supplier must perform its obligations meeting the requirements of:

- all applicable Law regarding health and safety
- the Buyer's current health and safety policy while at the Buyer's Premises, as provided to the Supplier

29.2 The Supplier must as soon as possible notify the other of any health and safety incidents or material hazards they're aware of at the Buyer Premises that relate to the performance of the Framework Contract.

30. Environment

30.1 When working on Site the Supplier must perform its obligations under the Buyer's current Environmental Policy, which the Buyer must provide.

30.2 The Supplier must ensure that Supplier Staff are aware of the Buyer's Environmental Policy.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

31. Tax

31.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. The Buyer cannot terminate the Framework Contract where the Supplier has not paid a minor tax or social security contribution.

31.2 Where the Charges payable under the Framework Contract are or are likely to exceed £5 million at any point during the relevant Framework Contract Period, and an Occasion of Tax Non-Compliance occurs, the Supplier must notify the Buyer of it within 5 Working Days including:

- the steps that the Supplier is taking to address the Occasion of Tax Non-Compliance and any mitigating factors that it considers relevant
- other information relating to the Occasion of Tax Non-Compliance that the Buyer may reasonably need

31.3 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under the Framework Contract, the Supplier must both:

- comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions
- indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Framework Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff

31.4 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its Framework Contract with the Worker contains the following requirements:

- the Buyer may, at any time during the Framework Contract Period, request that the Worker provides information which demonstrates they comply with Clause 31.3, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer
- the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers isn't good enough to demonstrate how it complies with Clause 31.3 or confirms that the Worker is not complying with those requirements
- the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management

32. Conflict of interest

32.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential Conflict of Interest.

32.2 The Supplier must promptly notify and provide details to the Buyer if a Conflict of Interest happens or is expected to happen.

32.3 The Buyer can terminate its Framework Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

33. Reporting a breach of the Framework Contract

33.1 As soon as it is aware of it the Supplier and Supplier Staff must report to the Buyer any actual or suspected breach of:

- Law
- Clause 12.1
- Clauses 27 to 32

33.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in Clause 33.1 to the Buyer or a Prescribed Person.

34. Resolving disputes

34.1 If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

34.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using Clauses 34.3 to 34.5.

34.3 Unless the Buyer refers the Dispute to arbitration using Clause 34.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

- determine the Dispute
- grant interim remedies
- grant any other provisional or protective relief

34.4 The Supplier agrees that the Buyer has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

34.5 The Buyer has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under Clause 34.3, unless the Buyer has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under Clause 34.4.

34.6 The Supplier cannot suspend the performance of the Framework Contract during any Dispute.

35. Which law applies

This Framework Contract and any issues arising out of, or connected to it, are governed by English law.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Schedule 1 (Definitions)

1.1 In the Framework Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.

1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.

1.3 In the Framework Contract, unless the context otherwise requires:

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

1.3.1 the singular includes the plural and vice versa;

1.3.2 reference to a gender includes the other gender and the neuter;

1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;

1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.3.5 the words "including", "other", "in particular", "for example" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "without limitation";

1.3.6 references to "writing" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

1.3.7 references to "representations" shall be construed as references to present facts, to "warranties" as references to present and future facts and to "undertakings" as references to obligations under the Framework Contract;

1.3.8 references to "Clauses" and "Schedules" are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;

1.3.9 references to "Paragraphs" are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided; and

1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified.

1.3.11 the headings in the Framework Contract are for ease of reference only and shall not affect the interpretation or construction of the Framework Contract; and

1.3.12 where the Buyer is a Crown Body it shall be treated as contracting with the Crown as a whole.

1.4 In the Framework Contract, unless the context otherwise requires, the following words shall have the following meanings:

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

"Achieve"	in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone and "**Achieved**", "**Achieving**" and "**Achievement**" shall be construed accordingly;
"Affected Party"	the party seeking to claim relief in respect of a Force Majeure Event;
"Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
"Annex"	extra information which supports a Schedule;
"Approval"	the prior written consent of the Buyer and "**Approve**" and "**Approved**" shall be construed accordingly;
"Audit"	the Buyer's right to: a) verify the accuracy of the Charges and any other amounts payable by the Buyer under a Framework Contract (including proposed or actual variations to them in accordance with the Framework Contract); b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services; c) verify the Open Book Data; d) verify the Supplier's and each Subcontractor's compliance with the applicable Law; e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Schedule 26 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Buyer shall have no obligation to inform the Supplier of the purpose or objective of its investigations; f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables; g) obtain such information as is necessary to fulfil the Buyer's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; h) review any books of account and the internal contract management accounts kept by the Supplier in connection with the Framework Contract; i) carry out the Buyer's internal and statutory audits and to prepare, examine and/or certify the Buyer's annual and interim reports and accounts;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Buyer has used its resources. a)
"Auditor"	a) the Buyer's internal and external auditors; b) the Buyer's statutory or regulatory auditors; c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; d) HM Treasury or the Cabinet Office; e) any party formally appointed by the Buyer to carry out audit or similar review functions; and f) successors or assigns of any of the above;
"Buyer Cause"	any breach of the obligations of the Buyer or any other default, act, omission, negligence or statement of the Buyer, of its employees, servants, agents in connection with or in relation to the subject-matter of the Framework Contract and in respect of which the Buyer is liable to the Supplier;
"BACS"	the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom;
"Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Framework Contract;
"Buyer Assets"	the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Framework Contract;
"Buyer Authorised Representative"	the representative appointed by the Buyer from time to time in relation to the Framework Contract initially identified in the Award Form;
"Buyer Premises"	premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them);
"Framework Contract"	the Framework Contract between the Buyer and the Supplier, which consists of the terms set out and referred to in the Award Form;
"Framework Contract Period"	the Framework Contract Period in respect of the Framework Contract;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

"Central Government Body"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
"Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Framework Contract which comes into force after the Start Date;
"Change of Control"	a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;
"Charges"	b) the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Framework Contract, as set out in the Award Form, for the full and proper performance by the Supplier of its obligations under the Framework Contract less any Deductions;
"Claim"	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Framework Contract;
"Commercially Sensitive Information"	the Confidential Information listed in the Award Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Buyer that, if disclosed by the Buyer, would cause the Supplier significant commercial disadvantage or material financial loss;
"Comparable Supply"	the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables;
"Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
"Confidential Information"	means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as **"confidential"**) or which ought reasonably to be considered to be confidential;
"Conflict of Interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to the Buyer under the Framework Contract, in the reasonable opinion of the Buyer;
"Framework Contract"	c) the Framework Contract to be entered into between the Buyer and the Supplier for the provision of the Deliverables;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

"Contracts Finder"	the Government's publishing portal for public sector procurement opportunities and contract data;
"Framework Contract Period"	the term of the Framework Contract from the earlier of the: a) applicable Start Date; or b) the Effective Date until the applicable End Date;
"Framework Contract Value"	the higher of the actual or expected total Charges paid or payable under the Framework Contract where all obligations are met by the Supplier;
"Framework Contract Year"	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
"Control"	control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly;
"Controller"	has the meaning given to it in the GDPR;
"Core Terms"	d) the Buyer's standard terms and conditions for common goods and services which comprise one part of the Framework Contract the full title of which is Core Terms – Mid-tier version 1.0;
"Costs"	the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables: a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Work Day, of engaging the Supplier Staff, including: i) base salary paid to the Supplier Staff; ii) employer's National Insurance contributions; iii) pension contributions; iv) car allowances; v) any other contractual employment benefits; vi) staff training; vii) work place accommodation; viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and ix) reasonable recruitment costs, as agreed with the Buyer; b) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets; c) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; and d) Reimbursable Expenses to the extent these have been specified as allowable in the Award Form and are incurred in delivering any Deliverables; but excluding: a) Overhead; b) financing or similar costs; c) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Framework Contract Period whether in relation to Supplier Assets or otherwise; d) taxation; e) fines and penalties; f) amounts payable under Schedule 12 (Benchmarking) where such Schedule is used; and g) non-cash items (including depreciation, amortisation, impairments and movements in provisions);
"Crown Body"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"CRTPA"	the Contract Rights of Third Parties Act 1999;
"Data Protection Impact Assessment	an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
"Data Protection Legislation"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of personal data and privacy; (iii) all applicable Law about the Processing of personal data and privacy;
"Data Protection Officer"	has the meaning given to it in the GDPR;
"Data Subject"	has the meaning given to it in the GDPR

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under the Framework Contract;
"Default"	any breach of the obligations of the Supplier (including abandonment of the Framework Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of the Framework Contract and in respect of which the Supplier is liable to the Buyer;
"Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
"Deliverables"	Goods and/or Services that may be ordered under the Framework Contract including the Documentation;
"Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of the Framework Contract as confirmed and accepted by the Buyer by the either (a) confirmation in writing to the Supplier; or (b) where Schedule 8 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. "**Deliver**" and "**Delivered**" shall be construed accordingly;
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable) for the period specified in the Award Form (for the purposes of this definition the **"Disaster Period"**);
"Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);
"Dispute"	any claim, dispute or difference arises out of or in connection with the Framework Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Framework Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in Clause 34 (Resolving disputes);
"Documentation"	descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals,

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under the Framework Contract as: a) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables b) is required by the Supplier in order to provide the Deliverables; and/or c) has been or shall be generated for the purpose of providing the Deliverables;
"DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions;
"Due Diligence Information"	any information supplied to the Supplier by or on behalf of the Buyer prior to the Start Date;
"Effective Date"	the date on which the final Party has signed the Framework Contract;
"EIR"	the Environmental Information Regulations 2004;
"Employment Regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;
"End Date"	the earlier of: a) the Expiry Date (as extended by any Extension Period exercised by the Buyer under Clause 10.2); or b) if the Framework Contract is terminated before the date specified in (a) above, the date of termination of the Framework Contract;
"Environmental Policy"	to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer;
"Estimated Year 1 Charges	the anticipated total Charges payable by the Buyer in the first Framework Contract Year specified in the Award Form;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

"Estimated Yearly Charges"	means for the purposes of calculating each Party's annual liability under clause 11.2 : i) in the first Framework Contract Year, the Estimated Year 1 Charges; or ii) in any subsequent Framework Contract Years, the Charges paid or payable in the previous Framework Contract Year; or e) f) iii) after the end of the Framework Contract, the Charges paid or payable in the last Framework Contract Year during the Framework Contract Period; g)
"Equality and Human Rights Commission"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Existing IPR"	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Framework Contract (whether prior to the Start Date or otherwise);
"Expiry Date"	the date of the end of the Framework Contract as stated in the Award Form;
"Extension Period"	such period or periods beyond which the Initial Period may be extended up to a maximum of the number of years in total specified in the Award Form;
"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
"Force Majeure Event"	any event, circumstance, matter or cause affecting the performance by either the Buyer or the Supplier of its obligations arising from: h) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Framework Contract; a) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; b) acts of a Crown Body, local government or regulatory bodies; c) fire, flood or any disaster; or d) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding:

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	i) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain; ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and iii) any failure of delay caused by a lack of funds;
"Force Majeure Notice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;
"Award Form"	the document outlining the Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and the Buyer;
" Incorporated Terms"	the contractual terms applicable to the Framework Contract specified in the Award Form;
" Special Terms"	any additional terms and conditions specified in the Award Form incorporated into the Framework Contract;
" Tender Response"	the tender submitted by the Supplier to the Buyer and annexed to or referred to in Schedule 4 (Tender);
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679)
"General Anti-Abuse Rule"	a) the legislation in Part 5 of the Finance Act 2013 and; and b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid National Insurance contributions;
"General Change in Law"	a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Goods"	goods made available by the Supplier as specified in Schedule 2 (Specification) and in relation to a Framework Contract as specified in the Award Form;
"Good Industry Practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
"Government"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

"Government Data"	the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Buyer's Confidential Information, and which: i) are supplied to the Supplier by or on behalf of the Buyer; or ii) the Supplier is required to generate, process, store or transmit pursuant to the Framework Contract;
"Government Procurement Card"	the Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-card--2;
"Guarantor"	the person (if any) who has entered into a guarantee in the form set out in Schedule 23 (Guarantee) in relation to this Framework Contract;
"Halifax Abuse Principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"HMRC"	Her Majesty's Revenue and Customs;
"ICT Policy"	the Buyer's policy in respect of information and communications technology, referred to in the Award Form, which is in force as at the Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;
"Impact Assessment"	an assessment of the impact of a Variation request by the Buyer completed in good faith, including: a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Framework Contract; b) details of the cost of implementing the proposed Variation; c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; d) a timetable for the implementation, together with any proposals for the testing of the Variation; and e) such other information as the Buyer may reasonably request in (or in response to) the Variation request;
"Implementation Plan"	the plan for provision of the Deliverables set out in Schedule 8 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

"Indemnifier"	a Party from whom an indemnity is sought under this Framework Contract;
"Independent Control"	where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and "**Independent Controller**" shall be construed accordingly;
"Indexation"	the adjustment of an amount or sum in accordance with the Award Form;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Information Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
"Initial Period"	the initial term of the Framework Contract specified in the Award Form;
"Insolvency Event"	a) in respect of a person: b) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or c) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or d) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or e) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or f) an application order is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or g) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or h) being a "small company" within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	i) where the person is an individual or partnership, any event analogous to those listed in limbs (a) to (g) (inclusive) occurs in relation to that individual or partnership; or j) any event analogous to those listed in limbs (a) to (h) (inclusive) occurs under the law of any other jurisdiction;
"Installation Works"	all works which the Supplier is to carry out at the beginning of the Framework Contract Period to install the Goods in accordance with the Framework Contract;
"Intellectual Property Rights" or "IPR"	a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information; b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and c) all other rights having equivalent or similar effect in any country or jurisdiction;
"Invoicing Address"	the address to which the Supplier shall Invoice the Buyer as specified in the Award Form;
"IPR Claim"	any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Buyer in the fulfilment of its obligations under the Framework Contract;
"IR35"	the off-payroll rules requiring individuals who work through their company pay the same tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies;
"Joint Controller Agreement"	the agreement (if any) entered into between the Buyer and the Supplier substantially in the form set out in Annex 2 of Schedule 20 (*Processing Data*);
"Joint Controllers"	where two or more Controllers jointly determine the purposes and means of Processing;
"Key Personnel"	the individuals (if any) identified as such in the Award Form;
"Key Sub-Contract"	each Sub-Contract with a Key Subcontractor;
"Key Subcontractor"	any Subcontractor: a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	b) which, in the opinion of the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or c) with a Sub-Contract with the Framework Contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under the Framework Contract, and the Supplier shall list all such Key Subcontractors in section 29 of the Award Form;
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;
"Law"	any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply;
"LED"	i) Law Enforcement Directive (Directive (EU) 2016/680)
"Losses"	all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in Framework Contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "**Loss**" shall be interpreted accordingly;
"Lots"	the number of lots specified in Schedule 2 (Specification), if applicable;
"Marketing Contact"	shall be the person identified in the Award Form;
"Milestone"	an event or task described in the Implementation Plan;
"Milestone Date"	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;
"Month"	a calendar month and "**Monthly**" shall be interpreted accordingly;
"National Insurance"	contributions required by the National Insurance Contributions Regulations 2012 (SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;
"New IPR"	a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of the Framework Contract and updates and amendments of these items including (but not limited to) database schema; and/or

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	b) IPR in or arising as a result of the performance of the Supplier's obligations under the Framework Contract and all updates and amendments to the same; but shall not include the Supplier's Existing IPR;
"Occasion of Tax Non – Compliance"	where: a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of: i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle; ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion;
"Open Book Data"	complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Framework Contract, including details and all assumptions relating to: a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables; b) operating expenditure relating to the provision of the Deliverables including an analysis showing: i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables; ii) manpower resources broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each manpower grade; iii) a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier Profit Margin; and

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	iv) Reimbursable Expenses, if allowed under the Award Form; c) Overheads; d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables; e) the Supplier Profit achieved over the Framework Contract Period and on an annual basis; f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier; g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and h) the actual Costs profile for each Service Period;
"Overhead"	those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs";
"Parliament"	takes its natural meaning as interpreted within by Law;
"Party"	the Buyer or the Supplier and "**Parties**" shall mean both of them where the context permits;
"Personal Data"	has the meaning given to it in the GDPR;
"Personal Data Breach"	has the meaning given to it in the GDPR;
"Prescribed Person"	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies;
"Progress Meeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;
"Progress Meeting Frequency"	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Award Form;
"Progress Report"	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;
"Progress Report Frequency"	the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Award Form;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

"Prohibited Acts"	a) to directly or indirectly offer, promise or give any person working for or engaged by the Buyer or any other public body a financial or other advantage to: i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity; b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with the Framework Contract; or c) committing any offence: i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii) under legislation or common law concerning fraudulent acts; or iii) defrauding, attempting to defraud or conspiring to defraud the Buyer or other public body; or d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;
"Protective Measures"	technical and organisational measures which must take account of: j) a) the nature of the data to be protected k) b)harm that might result from Data Loss Event; l) c) state of technological development m) d) the cost of implementing any measures including but not limited to pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it;
"Recall"	a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the IPR rights) that might endanger health or hinder performance;
"Recipient Party"	the Party which receives or obtains directly or indirectly Confidential Information;
"Rectification Plan"	the Supplier's plan (or revised plan) to rectify it's breach using the template in Schedule 25 (Rectification Plan Template) which shall include:

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	a) full details of the Default that has occurred, including a root cause analysis; b) the actual or anticipated effect of the Default; and c) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);
"Rectification Plan Process"	the process set out in Clause 10.4.2 to 10.4.4 (Rectification Plan Process);
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);
"Reimbursable Expenses"	the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including: a) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and b) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;
"the Buyer's Confidential Information"	c) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Buyer (including all Buyer Existing IPR and New IPR); d) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Buyer's attention or into the Buyer's possession in connection with the Framework Contract; and information derived from any of the above;
"Relevant Requirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010;
"Relevant Tax Authority"	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;
"Reminder Notice"	a notice sent in accordance with Clause 10.6 given by the Supplier to the Buyer providing notification that payment has not been received on time;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

"Replacement Deliverables"	any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables , whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Subcontractor"	a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);
"Replacement Supplier"	any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer;
"Request For Information"	a request for information or an apparent request relating to the Framework Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs;
"Required Insurances"	the insurances required by Schedule 22 (Insurance Requirements);
"Satisfaction Certificate"	the certificate (materially in the form of the document contained in Annex 2 of Part B of Schedule 8 (Implementation Plan and Testing) or as agreed by the Parties where Schedule 8 is not used in this Framework Contract) granted by the Buyer when the Supplier has Achieved a Milestone or a Test;
"Schedules"	any attachment to the Framework Contract which contains important information specific to each aspect of buying and selling;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to Schedule 16 (Security) (if applicable);
"Security Policy"	the Buyer's security policy, referred to in the Award Form, in force as at the Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
"Serious Fraud Office"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Service Levels"	any service levels applicable to the provision of the Deliverables under the Framework Contract (which, where Schedule 10 (Service Levels) is used in this Framework Contract, are specified in the Annex to Part A of such Schedule);
"Service Period"	has the meaning given to it in the Award Form;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

"Services"	services made available by the Supplier as specified in Schedule 2 (Specification) and in relation to a Framework Contract as specified in the Award Form;
"Service Transfer"	any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;
"Service Transfer Date"	the date of a Service Transfer;
"Sites"	any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; c) those premises at which any Supplier Equipment or any part of the Supplier System is located (where ICT Services are being provided)
"SME"	an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises;
"Special Terms"	any additional Clauses set out in the Award Form which shall form part of the respective Framework Contract;
"Specific Change in Law"	a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;
"Specification"	the specification set out in Schedule 2 (Specification), as may, in relation to the Framework Contract, be supplemented by the Award Form;
"Standards"	any: a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; b) standards detailed in the specification in Schedule 2 (Specification); c) standards detailed by the Buyer in the Award Form or agreed between the Parties from time to time;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	d) relevant Government codes of practice and guidance applicable from time to time;
"Start Date"	the date specified on the Award Form;
"Storage Media"	the part of any device that is capable of storing and retrieving data;
"Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than a Contract, pursuant to which a third party: a) provides the Deliverables (or any part of them); b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third Party appointed to process Personal Data on behalf of the Supplier related to the Framework Contract;
"Supplier"	the person, firm or company identified in the Award Form;
"Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Framework Contract but excluding the Buyer Assets;
"Supplier Authorised Representative"	the representative appointed by the Supplier named in the Award Form, or later defined in a Framework Contract;
"Supplier's Confidential Information"	a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier; b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier's attention or into the Supplier's possession in connection with the Framework Contract; c) Information derived from any of (a) and (b) above;
"Supplier's Contract Manager	the person identified in the Award Form appointed by the Supplier to oversee the operation of the Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment;
"Supplier Equipment"	the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Framework Contract;
"Supplier Non-Performance"	where the Supplier has failed to: a) Achieve a Milestone by its Milestone Date; b) provide the Goods and/or Services in accordance with the Service Levels ; and/or c) comply with an obligation under the Framework Contract;
"Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of the Framework Contract for the relevant period;
"Supplier Profit Margin"	in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under the Framework Contract;
"Supply Chain Information Report Template"	the document at Annex 1 of Schedule 18 Supply Chain Visibility;
"Supporting Documentation"	sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Framework Contract detailed in the information are properly payable;
"Termination Notice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate the Framework Contract on a specified date and setting out the grounds for termination;
"Test Issue"	any variance or non-conformity of the Deliverables or Deliverables from their requirements as set out in the Framework Contract;
"Test Plan"	a plan: a) for the Testing of the Deliverables; and b) setting out other agreed criteria related to the achievement of Milestones;
"Tests and Testing"	any tests required to be carried out pursuant to the Framework Contract as set out in the Test Plan or elsewhere in the Framework Contract and "**Tested**" shall be construed accordingly;
"Third Party IPR"	Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

"Transferring Supplier Employees"	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;
"Transparency Information"	the Transparency Reports and the content of the Framework Contract, including any changes to this Framework Contract agreed from time to time, except for – n) (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Buyer; and (ii) Commercially Sensitive Information;
"Transparency Reports"	the information relating to the Deliverables and performance pursuant to the Framework Contract which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Schedule 6 (Transparency Reports);
"Variation"	has the meaning given to it in Clause 24 (Changing the Framework Contract);
"Variation Form"	the form set out in Schedule 21 (Variation Form);
"Variation Procedure"	the procedure set out in Clause 24 (Changing the Framework Contract);
"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
"VCSE"	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
"Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables; and
"Working Day"	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Award Form.
"Work Day"	7.5 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day;
"Work Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Schedule 2 (Specification)

This Schedule sets out what the Buyer wants.

For all Deliverables, the Supplier must help the Buyer comply with any specific applicable Standards of the Buyer.

A. THE SPECIFICATION

Background

The FSA National Food Crime Unit (NFCU) has a remit to conduct criminal investigations, including the collection of evidence to prove that food crime has taken place and prosecute and convict offenders.

Evidence is increasingly stored on electronic media such as IT Servers, desktop and mobile computers, cloud applications, tablets and mobile phones.

The NFCU wishes to implement a Framework that includes a minimum of two and a maximum of four pre-qualified suppliers. The suppliers will provide digital forensic technicians and services to extract data from electronic media that is owned/operated by suspects and undertake preliminary analysis, to allow further analysis by NFCU investigators in a way that is compliant with the evidence capturing techniques.

As NFCU Investigations require a need to use digital forensic technicians and services, the team will call off services (work packages) by direct award from the framework qualified supplier that:

- Offers best value:
- Is accredited to do so,
- Has current capability to deliver;
- Is able to provide services to the stated UK Geographic area
- If appropriate; has the ability to extract data from the specific media types.

The supplier will provide the service as specified at the time.

From time to time, the NFCU may also ask suppliers to provide emerging technology awareness to NFCU investigators that enables them to identify technology platforms that may be used by criminals to store and manage data.

The supplier should note that been on the framework does not guarantee work. This will be dependent on the FSA’s requirements.

No call off can be put in place less than 2 months before the framework expires. It should be noted that attendance at court may take several months or years. The call off will remain open until this is completed.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

The Specification

It is difficult for us anticipate the precise future requirements; however, we expect your response to cover the following areas: -

On premise Imaging and Analysis

The supplier will attend the premises together with an NFCU investigator and seize or copy any digital media found/ carry out forensic imaging and digital media removal.

The supplier will transport data and digital media to their site and conduct data analysis based on the work package, generating a reporting system which includes documentation which complies with CPIA obligations. They will provide the data after a word search in a format that can be viewed and evaluated by NFCU Investigators simultaneously based at multiple site.

Please note any forensic technicians attending searches on suspects premises will be provided with the correct PPE kit by the NFCU Investigator. This must be worn at all times and as specified by the Investigator, for example, food preparation areas will require wellington boots, overalls and hard hats to be worn.

Criminal Procedure and Investigation Act (CPIA) 1996

The supplier's forensic analysts should have a firm understanding that post the initial imaging and analysis, they should have a continuing commitment to assist with the CPIA Disclosure process going forward.

Service Level

The supplier will respond to an order within 48 hours of receipt to confirm timescales.

Assumptions

General assumptions include:

- NFCU will ensure proper legal authorisation is in place to allow the supplier to carry out imaging and analysis of material.
- NFCU will ensure that all relevant intelligence is communicated to the supplier to facilitate proper analysis of material.
- NFCU will provide the supplier with timely input to their analysis.
- The anticipated date and time that the Imaging will take place at the suspects premises.

Analysis will be carried out during working hours (Mon-Fri 09:00-17:30 excluding Bank Holidays)

The Provider will be expected to:

- Attend court as a professional witness as and when required.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- Attend crime scenes of all descriptions including abattoirs and meat processing factories to search and recover digital media with a minimum of 72 hours' notice from the first point of contact with the NFCU.
- Have the ability to recover and examine digital data from vehicles and associated devices such as satellite navigation systems, or to be able to liaise with the relevant manufacturer to produce an evidential product for the NFCU Investigator.

- Have the ability to recover and examine digital data from labelling / printing machines and associated software, or to be able to liaise with the relevant manufacturer to produce an evidential product for the NFCU investigator.

- Have the ability to attend scenes / premises both commercial and private dwellings to capture and preserve data from complex and large IT systems and infrastructures, i.e. on-site servers and systems.

- Have the ability to capture and preserve digital data (Forensic Copy/Image) of conventional hard drives, internal and external computer hard disks, memory stick, USB devises and extract the data for analysis.

- Conduct a word search supplied by NFCU Investigators to target relevant materiel stored on the recovered / imaged digital material.

- Have the ability to separate Legal Professional Privilege material generated during the word search to viewed by independent counsel.

- Provide a pricing structure and mechanism that clearly states charges prior to work being carried out.

- Demonstrate a process/ mechanism for management approval by the NFCU prior to work being commenced.

For the NFCU to review and present digital evidence to a court of law it is imperative that digital forensic work is carried out by an organisation who has achieved ISO17025 accreditation at a minimum of:

- Capture and preservation of digital data (Forensic Copy) of Conventional hard drives, internal and external computer hard disks, memory stick, USB devises.
- Extraction and analysis of data from digital media associated with MS Windows.

Please include a list of all other processes in which ISO17025 accreditation has been achieved e.g.

- ISO 17025 Accreditation in Logical capture and preservation of data from mobile phones, tablets, SIM cards – Please list the operating systems

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- ISO 17025 Accreditation in Physical capture and preservation of data from mobile phones, tablets, SIM cards – Please list the operating systems
- ISO 17025 Accreditation in Extraction and analysis of data associated with Apple and Linux

The NFCU operates from several different sites based throughout the UK as well as home working, therefore it is essential that a suitable reviewing platform is required to enable Investigators from multiple locations to be able to work on the same investigation.

Please give details of the reviewing platform used and how this will achieve the above.

As it is difficult to anticipate future requirements, as well as responding to the above criteria, bidders are asked to provide a technical and commercial (pricing) response to the following scenario.

Scenario for Evaluation Purposes

- A National Meat Supply business is suspected of extending ‘use by’ dates and supplying their customers with South American beef but labelling it as British beef.
- After Meat Hygiene Inspectors make unannounced visits the incident is passed to the National Food Crime Unit (NFCU) to investigate as a suspected fraud.
- A warrant is planned to be executed on the business headquarters (which is not a processing factory) with a view to seizing digital data from 2 servers situated on the premises.
- Further warrants are planned at 2 of the factories which also have a server in each one.
- It is known that the business runs off a ‘windows’ operating system, as well as a database which digitally sends information to labelling machines situated within the business factories. The business also runs an advertising department which operates on an ‘Apple’ Operating System.
- The warrants and various arrests produce several items that will require examination by a digital forensic department and put into a format that the NFCU Investigation team can view the end results.
- Below is a list of the data sizes that are recovered from the servers

Asset Tag	Date Received	Data Type	HDD Folder Name / Description	Compressed Image Size (GB)	Uncompressed Size (GB)	Data Accessible

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

		Server	Location 1 Server 1	21.5	23.6	Yes
		Server	Location 1 Server 2	40.3	111.6	Yes
		Server	Location2 Server 1	9.9	11.2	Yes
		Server	Location 2 Server 2	8.2	N/A - not accessible yet	No
		NAS Backup	Location 1 NAS	68	N/A - not accessible yet	No
		NAS Backup	Location 2 NAS	28.6	N/A - not accessible yet	No
		Server	HQ Email Server Exchange	496	812.1	Yes
		Server	HQ File Server Share	121	172.5	Yes
		Financial System	Restored backup of Chorus financial system	6	N/A - not accessible yet	No

- The NAS files are believed to be data that is used to digitally send information to the labelling machines within the factories. These will need copying and put into a format that can be read by the labelling company to replicate the labelling system used by the business.
- The majority of the data is emails, excel documents, word documents and PDF's.

5 x Company Directors (including the Marketing Director) are arrested and the following list of digital media devices are recovered. These will require examination and puting into a format for the NFCU Investigations team to view:

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

4 x Samsung Galaxy S10 Mobile phones

1 x iPhone XS mobile phone

4 x Lenovo Think Pad T480 Laptops

1 x MacBook Pro 16inch 512GB

3 x iMac 27inch with 1 TB SSD

2 x 3TB external storage

Your technical response should address and include the following: -

1. What if any accreditation does your unit have for scene work, and if there is no accreditation in place are you working towards ISO17020, if so when do you believe this will be achieved?

2. What measures do you put in place for subsequent transportation and storage of exhibits seized?

3. What exhibiting data standards do you use?

4. What platform / format will the result be presented in? This will need to be viable for several NFCU investigators to work on at the same time from multiple locations including some home workers.
5. What form of data storage is supplied i.e. returned to NFCU on external hard drives, stored on a server with relevant costs?

6. How are the relevant exhibits identified by the NFCU from the data review presented to the courts? What is your ability to attend court and supply expert witnesses' evidence? Will the NFCU have to request the DFU to print out exhibits or prepare them in a readable / printable format for court; or will the NFCU be able to perform this function?

7. What is the scope of the ISO17025 accreditation held?

8. If a process or piece of work is not covered by ISO17025 will the NFCU be informed prior to commencement of the work?

9. What is the submission process?

10. What stages is the NFCU informed of the progress of the examination?

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

11. What are the time scales for the examination?

12. Is there a process to halt the examination once started and are there penalty costs involved?

13. The team will order services (work package) by direct award from the framework qualified supplier. Explain how you envisage the order service (work package) process working?

14. What are the qualifications and experience of the reporting technicians and the process for listing all persons who have an input into the examination?

15. What is the triage process and subsequent workflow including sign off by NFCU management?

Your commercial response should include: -

16. The estimated cost to attend the scenes and mirror the servers in question?
17. The total cost?
    This must include a full breakdown of the costs for the above work to be completed including but not limited to;
    - Triage costs
    - Examination costs
    - Subsequent statements, reports, storage and court appearance

18. Tenderers should include a rate card detailing the maximum day rates for roles including their grade and expertise.

Schedule 3 (Charges)

1. How Charges are calculated

2. The Framework Prices:

3. will be used as the basis for the charges (and are maximums that the Supplier may charge) under each Work Package Call Off; and

4.

4.1 The Charges:

4.1.1 shall be calculated in accordance with the terms of Work Package Call Off;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

4.2 Any variation to the Charges payable under a Work Package Call Off must be agreed between the Supplier and the Buyer and implemented using the procedure set out in this Schedule.

5. The pricing mechanisms

5.1 The pricing mechanisms and prices set out in Annex 1 shall be available for use in calculation of Charges in the Work Package Call Off.

6. Are costs and expenses included in the Charges

6.1 Except as expressly set out in Paragraph 4 below, or otherwise stated in the Award Form the Charges shall include all costs and expenses relating to the provision of Deliverables. No further amounts shall be payable in respect of matters such as:

6.1.1 incidental expenses such as travel, subsistence and lodging, document or report reproduction, shipping, desktop or office equipment costs, network or data interchange costs or other telecommunications charges; or

6.1.2 costs incurred prior to the commencement of the Work Package Call Off.

7. When the Supplier can ask to change the Framework Charges

7.1 The Charges will be fixed for the first **2 (Two)** years following the Framework Contract Commencement Date (the date of expiry of such period is a "**Review Date**"). After this Charges can only be adjusted on each following yearly anniversary (the date of each such anniversary is also a "**Review Date**").

7.2 The Supplier shall give the Buyer at least three (3) Months' notice in writing prior to a Review Date where it wants to request an increase. If the Supplier does not give notice in time then it will only be able to request an increase prior to the next Review Date.

7.3 Any notice requesting an increase shall include:

7.3.1 a list of the Framework Prices to be reviewed;

7.3.2 for each of the Framework Price under review, written evidence of the justification for the requested increase including:

8. Other events that allow the Supplier to change the Charges

8.1 The The Framework Prices can also be varied (and Annex 1 will be updated accordingly) due to:

8.1.1 a Specific Change in Law in accordance with Clause 24;

8.1.2 a review in accordance with insurance requirements in Clause 13;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

8.1.3 a request from the Supplier, which it can make at any time, to decrease the Charges; and

8.1.4 5.1.5 if Paragraph 7 is not used]

indexation, where Annex 1 states that a particular Charge or any component is "subject to Indexation" in which event Paragraph 7 below shall apply.]

9. When you will be reimbursed for travel and subsistence

9.1 Expenses shall only be recoverable where:

9.1.1 the Time and Materials pricing mechanism is used; and

9.1.2 the Work Package Call Off states that recovery is permitted; and

9.1.3 they are Reimbursable Expenses and are supported by Supporting Documentation.

9.2 The Buyer shall provide a copy of their current expenses policy to the Supplier upon request.

Annex 1: Rates and Prices

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Food Standards Agency
food.gov.uk

Status: REVISED

Application form for a project with the Food Standards Agency Financials Template

All tabs except the rate card should be completed with the costs relating to the scenario given in the specification.

The rate card should show the maxium cost for each role for the life of the Framework Agreement.

Applicants should complete each part of this application as fully and as clearly as possible

Brief instructions are given in the boxes at the start of each section.
Some boxes have **blue** text and this indicates that the value is calculated automatically
Some boxes are shaded **red** and these boxes **must** be completed

Guidance notes on completion of fields can be removed from view by pressing the ESC key

Please submit the application through the Agency's electronic Public Procurement System (Bravo) by the deadline detailed on the Bravo system

This form should be completed by the project lead applicant and must include the collated costs for all participating organisations applying for the project work

Tender Reference	FA900084

Tender Title	Framework for Digital Forensic Service Providers

Full legal organisation name	CCL-Forensics Ltd

Main contact title	Miss
Main contact forname	Samantha
Main contact surname	Ollis

Main contact position	Internal Account Manager and Bid Writer
Main contact email	sam.ollis@cclgroupltd.com
Main contact phone	07534 637 708

Will you charge the Agency VAT on this proposal?	Yes
Please state your VAT registration number:	GB218593487

Project Costs Summary Breakdown by Participating Organisations

Please include only the cost to the FSA.

Organisation	VAT Code*	Total (£)
CCL-Forensics Limited	STD	£ 34,956.00
Insert name of Organisation 2	Please select	£ -
Insert name of Organisation 3	Please select	£ -
Insert name of Organisation 4	Please select	£ -
Insert name of Organisation 5	Please select	£ -
		£ -
		£ -
		£ -
Total Project Costs (excluding VAT) **		**£ 34,956.00**

* Please indicate zero, exempt or standard rate. VAT charges not identified above will not be paid by the FSA
** The total cost figure should be the same as the total cost shown below and in the Schedule of payments tab.

Project Costs Summary (*Automatically calculated*)

Staff Costs	**£**	**27,580.00**
Overhead Costs	**£**	**-**
Consumables and Other Costs	**£**	**7,376.00**
Travel and Subsistence Costs	**£**	**-**
Other Costs - Part 1	**£**	**-**
Other Costs - Part 2	**£**	**-**
Other Costs - Part 3	**£**	**-**
Other Costs - Part 4	**£**	**-**
Other Costs - Part 5	**£**	**-**
Total Project Costs	**£**	**34,956.00**

COST OR VOLUME DISCOUNTS - INNOVATION
The Food Standards Agency collaborates with our suppliers to improve efficiency and performance to save the taxpayer money. A tenderer should include in his tender the extent of any discounts or rebates offered against their normal day rates or other costs during each year of the contract. Please provide full details below:

SIGNATURE		
NAME		
DATE		
REVISION DATE	11-Aug-2020	Enter the effective date if this version of the template replaces an earlier version

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Food Standards Agency
food.gov.uk

Staff Costs Table

*This should reflect details entered in your technical application section 4C.
Please insert as many lines as necessary for the individuals in the project team.
Please note that FSA is willing to accept pay rates based upon average pay costs. You will need to indicate where these have been used.

* Role or Position within the project	Participating Organisation	Daily Rate (£/Day)	* Daily Overhead Rate(£/Day)	Days to be spent on the project by all staff at this grade	Total Cost (incl. overheads)
Principal Analyst (Data Analytics)	CCL-Forensics	£ 1,040.00		1.25	£ 1,300.00
Analyst (PC)	CCL-Forensics	£ 760.00		6	£ 4,560.00
Analyst (Mobile)	CCL-Forensics	£ 760.00		3.75	£ 2,850.00
Analyst (Data Analytics)	CCL-Forensics	£ 760.00		6.25	£ 4,750.00
Technician (Data Analytics & PC)	CCL-Forensics	£ 640.00		6.25	£ 4,000.00
Senior Analyst (On Site)	CCL-Forensics	£ 880.00		5.25	£ 4,620.00
Senior Analyst (Data Analytics)	CCL-Forensics	£ 880.00		6.25	£ 5,500.00
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
			Total Labour Costs		£ 27,580.00
			* Total Overhead Costs (if not shown above)		

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Consumable/Equipment Costs

Please provide a breakdown of the consumables/equipment items you expect to consume during the project

Item	Quantity	Cost/Item(£)	Total
Nuix Usage Charge	1	£ 3,750.00	£ 3,750.00
Azure Data Hsoting	1	£ 150.00	£ 150.00
Reviewer User Licenses	2	£ 1,738.00	£ 3,476.00
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -

Total Material Costs	£ 7,376.00

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Travel and Subsistence Costs

Please provide a breakdown of the travel and subsistence costs you expect to incur during the project

Purpose of journey or description of subsistence cost	Frequency	Cost each (£)	Total Cost
Travel and subsistence are hard to estimate when no lo		£ -	£ -
Mileage @ 0.55p per mile to be taken from CCL's Strat		£ -	£ -
Subsistence. Capped @ £25.50 when away from place		£ -	£ -
Hotel allowance £80 per night (£100 per night in Londo		£ -	£ -
Given CCL's central location accommodation costs are		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -

Total Travel and Subsistence Costs	£ -

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Food Standards Agency
food.gov.uk

The Pricing Schedule

Please complete a proposed schedule of payments below, **excluding VAT** to be charged by any subcontractors to the project lead applicant. This must add up to the same value as detailed in the Summary of project costs to FSA including participating organisations costs.

Where differing rates of VAT apply against the deliverables please provide details on separate lines.

Please link all deliverables (singly or grouped) to each payment. Please ensure that deliverable numbers are given as well as a brief description e.g. Deliverable 01/02: interim report submitted to the FSA, monthly report, interim report, final report

Payment will be made to the Contractor, as per the schedule of payments upon satisfactory completion of the deliverables.

Proposed Project Start Date	**20-Jul-2020**	**Amount**				
Invoice Due Date	**Description as to which deliverables this invoice will refer to (*Please include the deliverable ref no(s) as appropriate*)**	***Net**	**** VAT Code**	**§ Duration from start of project (Weeks)**	**§ Duration from start of project (Date)**	**Financial Year**
31-Jul-2020	Identification and Preservation	£ 9,817.50	STD	2	31-Jul-2020	2020-21
31-Aug-2020	Collection, processing, analysis and review	£ 20,531.00	STD	6	31-Aug-2020	2020-21
30-Sep-2020	Production and project completion	£ 4,607.50	STD	10	30-Sep-2020	2020-21
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				
		£ -				

Total	£ 34,956.00	Totals Agree

* Please insert the amount to be invoiced net of any VAT for each deliverable
** Please insert the applicable rate of VAT for each deliverable
§The number of weeks after project commencement for the deliverable to be completed

Summary of Payments

	Year 1	Year 2	Year 3	Year 4	
Financial Year (Update as applicable in YYYY-YY format)	2020-21	2019-20	2020-21	2021-22	Total
Total Amount	£ 34,956.00	£ -	£ 34,956.00	£ -	£ 69,912.00

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Food Standards Agency
food.gov.uk

Rate Card

The rate card should show the maximum rate for the staff role or position for the life of this Framework Agr

Role or position	Maximum Hourly Rate	Maximum Daily Rate	Daily Overhead rate
Technician - Mobile	£ 80.00	£ 640.00	£ 51,200.00
Analyst - Mobile	£ 95.00	£ 760.00	£ 72,200.00
Senior Analyst - Mobile	£ 110.00	£ 880.00	£ 96,800.00
Principal Analyst - Mobile	£ 130.00	£ 1,040.00	#########
Technician - PC/Data Analytics	£ 80.00	£ 640.00	£ 51,200.00
Analyst - PC/Data Analytics	£ 95.00	£ 760.00	£ 72,200.00
Senior Analyst - PC/Data Analytics	£ 110.00	£ 880.00	£ 96,800.00
Principal Analyst - PC/Data Analytics	£ 130.00	£ 1,040.00	#########
Principal Analyst, R&D	£ 160.00	£ 1,280.00	#########
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Schedule 4 (Tender)

Tender Application form for a project with the

- Applicants should complete each part of this application as fully and as clearly as possible
- Brief instructions are given in the grey boxes at the start of each section.
- Please submit the application through the Agency's eSourcing Portal (Bravo) by the deadline set in the invitation to tender document.

Lead Applicant's details

Surname	Ollis	First Name	Samantha	Initial	L	Title	Miss
Organisation	CCL-Forensics Ltd	Department	Bid Management				
Street Address	36 Cygnet Court						
Town/City	Stratford-upon-Avon	Country	Warwickshire	Postcode	CV37 9NW		
Telephone No	01789 261200	E-mail Address	Sam.ollis@cclgroupltd.com				

Is your organisation is a **small and medium enterprise**. (EU recommendation 2003/361/EC refers http://www.hmrc.gov.uk/manuals/cirdmanual/cird92800.htm	Yes		No	

TENDER SUMMARY

Framework for Digital Forensic Service Providers in England and Wales

	01/09/2020		1/09/2022-24

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

1: delivery of the requirements For THe FRAMEWORK AGREEMENT

A. TENDER SUMMARY

Please give a brief summary of the proposed work in no more than 400 words.

The world's major public sector organisations and best companies rely on CCL's digital investigation expertise. Integrating digital forensics, data analytics, data governance and cyber security has allowed us to become their trusted data partner, charged with finding, protecting and transforming data across law enforcement, legal and corporate settings.

Under the leadership of the former Director General of the National Crime Agency (NCA), CCL has grown its capacity and footprint, and is increasingly an intrinsic part of complex criminal, civil and commercial investigations.

CCL started providing digital forensic services to the Metropolitan Police in 2001 and is a long-standing partner of the National Crime Agency, UK police forces and HMRC. We support large-scale, sensitive investigations including counter terrorism, serious organised crime, child abuse, and fraud.

Our forensic experts, using proprietary solutions, provide you with complete confidence in the collection and analysis of digital material. Our role is to enable you to present an accurate scenario with no missing data, using collection methods that meet the widest range of accreditations of any UK digital forensic laboratory.

Computer Forensics: CCL's dedicated PC analysis laboratory perform forensic examinations on a wide range of computers and digital storage devices. As well as utilising standard commercial tools, CCL has advanced techniques and scripts to acquire data not usually accessible.

Mobile Devices: CCL's mobile device laboratory performs forensic examinations on thousands of mobile devices a year including mobile telephones, SIM and memory cards, tablets, satnavs, smart devices, drones and vehicle telematics systems. As well as utilising standard commercial tools, CCL has advanced engineering techniques to tackle unsupported devices and applications.

Data Analytics: CCL has a highly experienced Data Analytics team built on the fundamentals of digital forensics, responsible for the project management, processing, filtering, facilitation of review and production of data. Our solution allows us to process data quickly and intelligently and makes data available for review by investigators, whilst providing an audit at all stages. It can scale to meet large or small demands providing the ability for multiple investigators to review all data in one platform.

This proposal is intended to illustrate that CCL is comprehensively qualified to meet the Food Standards Agency's needs. We have achieved this by fully scoping the scenario provided as if it were a genuine engagement. Providing the FSA the

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

assurance that the methodology and costs accurately reflect those that would be provided should CCL be appointed. 397 words

B. Named Staff Members who will work on THE FRAMEWORK and Details of their Specialism and expertise

For each participating organisation on the project team please list:- the names and grades of all staff who will work on the project together with details of their specialism and expertise, their role in the project and details of up to 4 of their most recent, relevant published peer reviewed papers (where applicable). If new staff will be hired to deliver the project, please detail their grade, area/(s) of specialism and their role in the project team.

Lead Applicant	CCL-Forensics Limited

Named staff members, details of specialism and expertise.

CCL currently has the following staff numbers that can be drawn on to serve the NFCU:

4 Imaging Technicians

22 PC Analysts

37 Mobile Device Analysts

8 Data Analytics Analysts/Consultants

8 Cell Site Analysts

4 Research and Development

6 Forensic Case Officers

We have provided profiles that offer a cross section of experience levels and disciplines.

All staff engaged in digital forensics are educated to degree level or higher or have experience working with information systems. Analysts are from a variety of backgrounds, Law Enforcement and corporate and civil investigations, enabling us to bring a wide spectrum of investigative skills to casework

Data Analytics Analysts, PC Analysts and Imaging Technicians: All CCL analysts undergo a programme of training to enable them to acquire and maintain the skills and knowledge necessary to conduct forensic analysis. This includes: an initial induction programme, an assessment of training needs, access to learning resources, attendance at external or internal training courses, shadowing an experienced analyst assigned as their mentor and practical assignments. On

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

successful completion of the programme, trainees undertake a competency test. This is marked by a senior analyst, technical manager or other designated member of the team. An assessment of continued competence is tested every two years. Additionally, performance is monitored with consideration given to any non-conformances, observations or feedback given by the analyst's peers, mentor, line manager, customers or colleagues. When new technical methods are rolled out that are relevant to the analyst's role, the individual will receive further training and competency testing appropriate to the new or updated method. CCL maintains records of relevant authorisations, competence, education and professional qualifications, training, skills and experience and court attendances on our CCL Personnel system.

Mobile Device Analysts: CCL's training and initial competency consist of a six-week intensive programme whereby new starters undergo a combination of theory/classroom sessions, practice cases and competency assessments. Competency assessment is based on three different mobile phones and assesses the Analyst's ability to work to CCL's SOPs, work instructions and policies. Tests on iOS, Android and a basic mobile phone platform are assessed so the trainee builds experience in examination of basic devices such as SIM, memory cards and standard 'telephony' only devices. Progression onto the popular smartphone platforms trains the Analyst in managing large datasets, features of smart devices and the variety of raw artefacts used to store smartphone application data. Experienced hires undergo a streamlined structure of classroom and practice training, with a three-device competency test being sat when ready. Analysts are not permitted to work independently on casework until all three competency tests have been passed. Initial competency lasts for 1 year before being continually renewed every 2 years thereafter.

We currently have 18 analysts who have completed their classroom and hands on training and are operating as trainees within the lab.

Participant Organisation 1	
Named staff members, details of specialism and expertise.	
Participant Organisation 2	
Named staff members, details of specialism and expertise.	
Participant Organisation 3	
Named staff members, details of specialism and expertise.	

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

C. PARTICIPATING ORGANISATIONS' PAST PERFORMANCE

Please provide evidence of up to three similar projects that the project lead applicant and/or members of the project team are currently undertaking or have recently completed. Please include:

- The start date (and if applicable) the end date of the project/(s)
- Name of the client who commissioned the project.
- Details of any collaborative partners and their contribution
- The value
- A brief description of the work carried out.
- How the example(s) demonstrate the relevant skills and/or expertise.

What skills the team used to ensure the project (s) were successfully delivered.

National Crime Agency

Start Date: 1st October 2014

End Date: Jan 2023 (second contract awarded in Jan 2019)

Contact: Paul Daniels, Forensic Technical Lead/External Service Delivery Manager, Paul.daniels@nca.x.gsi.gov.uk

Value: £10-12m (current framework)

Services: As part of a framework of three providers, CCL holds a nationwide contract with the NCA for forensic recovery, examination, identification and interpretation of digital evidence and cell site analysis.

Includes 24x7x365 provision for on-site scene activity

Analysis is undertaken to Critical (24 hours), Urgent (7 days) or Standard (28 days) TRTs for approximately 1,200 submissions per annum.

Findings are provided to the NCA to Criminal Justice System evidential standards with provenance and evidential material, including witness statements and disclosure schedules. CCL attends criminal justice proceedings as required.

Services are provided in compliance with ISO17025 accreditation, the Regulator's Code of Conduct and ACPO guidelines. Analysis is carried out using tools and methodologies validated to ISO17025 by staff trained, assessed, security cleared and authorised.

CCL has provided client specific Standard Operating Procedures (SOPs) for NCA, which instructs on the use and operation of all software and equipment, and the handling and preparation of items for analysis.

Analysis is performed at varying levels according to requirements, ranging from information only download of data from mobile devices to full extraction, forensics analysis, provenance and interpretation of data for complex investigations.

Data is provided for review online, on external media or at CCL's dedicated viewing facility.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

CCL provides Cell Site Analysis, including analysis and interpretation of network data with other information (e.g. survey results or terrain mapping). Survey and desktop analysis responds to queries concerning all UK networks. Desktop analysis includes plotting locations of masts and locations of interest, with commentary or visual representation of anticipated service areas of cells. Complex data interpretation requiring assessment of likelihood is only performed by examiners with relevant experience.

A collection and delivery service is provided by security cleared drivers, vehicles are trackable online. Exhibits are receipted and tracked via an in-house tracking system that assures continuity of evidence and that exhibits cannot be lost or confused. Storage is in a purpose-built secure evidence store.

In addition to standard digital forensic services, CCL provides specialist case work, including knowledge of the Dark Web and Crypto Currency and a number of projects utilising Nuix to assist with Big Data Analysis.

CCL has a dedicated NCA contract management team, who attend contract review meetings, provide detailed weekly and monthly management information

Partners: Occasionally submitted devices have requirements for trace or DNA evidence, CCL maintains a sub-contact relationship with Eurofins for the provision of these services

Expertise: The delivery of services to the NCA requires all expertise in all areas required by the FSA.

- The full range of digital forensics services, provided to CJS evidential standards
- ISO17025 accreditation and the forensic regulator's codes
- Full contract management service

The Pension Regulator

Background: CCL were engaged by the Pension Regulator who were investigating offences relating to breaches of various financial regulations. All computers, servers, network storage, removable media and mobile phones were subject to collections, but no prior knowledge of the number of devices or capacity of storage was available.

Instructions:

- We were asked to attend three geographic sites to support Agency investigators in the simultaneous execution of three warrants. The sites included two domestic premises and one busy commercial premise.
- During the execution of the warrants, out teams were tasked to collect data responsive to the requirements of the investigation and make that data available for review by the investigation team and others.
- The warrants carried significant restrictions, specifically prohibiting the normal 'seize and sift' approach. This meant that we could not simply image media for later processing in our laboratories.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

- We were asked if we had a methodology that allowed us to perform the following actions on site.
    - identify all responsive materials
    - exclude any legally privileged materials.
    - Create a legally and forensically defensible export of the respondent data for uploading to an online review platform.

- The exception to the above restrictions was the processing of mobile phones and OUTLOOK PST/OST containers which could be acquired on-site and post processed in our labs.

- We were further asked if this task could be performed in the shortest timescale and with the absolute minimum disruption to the target business.

Services: Two staff were deployed to one town where one domestic and the commercial premises were located and a third member of the team was deployed to a second town. All team members were accompanied by Agency investigators.

To achieve the detailed and challenging warrant objectives, the team were equipped with rugged SPEKTOR laptops configured with SPEKTOR triage, SPEKTOR rapid imaging and SPEKTOR analysis software plus mobile phone tools. The two-man team tasked with the domestic and commercial premises were equipped with six SPEKTOR units mobile phone capability and the team member at the second domestic premises carried one SPEKTOR unit and a mobile phone capability.

In a co-ordinated action, the two geographically dispersed domestic premises were entered at 07:00hrs. In conjunction with the Agency investigators, a search of one premise resulted in two mobile phones, one laptop and six USB storage devices being targeted for processing.

One SPEKTOR unit was deployed to triage the contents of the laptop and a second SPEKTOR unit was deployed to triage the removable USB storage devices. The triage scope was to identify and process all user generated files such as office documents, archive files, email, images, social media, chat and web browser activity along with comprehensive system details.

Using multiple keyword lists, both responsive and LPP material was quickly identified, tagged and the permitted responsive data was exported onto an external USB disk together with a comprehensive ‘load file’ schedule and full forensic audit trail. Simultaneously, the two mobile phones were acquired using the mobile phone capability with the results stored on an external USB disk. Both disks were sealed in evidence bags and all paperwork finalised.

The forensic tasks completed at approximately 09:30 and the CCL team then assisted the Agency investigators in a final review of the premises to help identify any further digital devices of interest.

The CCL team and the Agency investigators then travelled a few miles to the commercial premises where further Agency investigators were waiting. An initial survey of the premises identified 26 computers of varying brands, a server, some network storage, approximately 45 removable USB storage devices and five mobile phones.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Starting at approximately 11am The team of two deployed all six SPEKTOR units and used the same triage setting and methodology to acquire, process and export just the respondent data to USB disks. All data was acquired, processed and exported onsite by 22:30 in compliance with the warrant and instructions.

Processing of data on the second domestic premises was initially delayed by the absence of the property owner but, once they arrived later in the day, a mobile phone and a computer were processed using the same methods.

Upon return to our laboratory next morning, all collected data including that permitted to be processed offsite was processed consolidated into a format suitable for importing to the clients hosted Relativity review platform.

Summary:

- Three premises, 28 computers, 51 USB storage devices, 1 server, 4TB network storage and 8 mobile phones.
- The clients warrant excluded the traditional seize and sift forensic approach and required advanced processing of data onsite.
- CCL team of three used SPEKTOR units and mobile phone tools to Triage, identify and exclude LPP materials and export responsive data
- All onsite forensic actions completed in one day, commencing at 07:00 and concluding at 22:30
- All follow up forensic actions were completed in a working day.
- Using SPEKTOR onsite not only met the restrictive warrant conditions but also saved client approximately 5-8 mandays of laboratory processing time and costs.

Expertise: This case study illustrates our experience in onsite investigations and the impact that our triage methodology and tools can have reducing laboratory time and costs

City of London Police

Start Date: November 2016

End Date: June 2019

Contact: Andrew Thompson, Detective Inspector Fraud Team, andrew.thompson@city-of-london.pnn.police.uk

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Value: £85,700

In 2016, City of London Police requested assistance from CCL for assistance in the management and organisation of a wealth of digital material that required reviewing. The following workflow was developed and deployed to assist the client with their investigatory and disclosure requirements:

Milestone 1: Collection, Processing and Searching

- A forensically secure collection and acquisition of the original exhibits was performed by CCL. Copies of the forensic images acquired by third parties were verified
- To facilitate review, data was extracted from the acquired forensic images and processed to create a single database. CCL used Nuix Workstation to achieve this result. The benefits being:
    - Identification of over 500 file types and data structures, including support for deleted file recovery and carving from unallocated space
    - Easy removal of files relating to the operation of the exhibits' systems, software and applications reduces the likelihood of irrelevant material being released for investigator review
    - Processing of complex files types and all emails identified on the devices without the need for further interaction or use of third-party tools

Milestone 2: Searching and Filtering

Upon formulation of a search strategy and agreement from the client, the data set were searched and filtered for a wide range of criteria, such as priority exhibits or exhibits from a certain premises, specific types of file or material, key dates or date ranges, and keywords or phrases. Nuix allowed the facilitation of:

- Identification and removal of duplicate files across all exhibits whilst maintaining metadata from duplicates, meaning investigators could assess the material efficiently whilst retaining the information required to identify connections between data sources
- Enabled collaborative online review by the entire case team, from any location, with senior officers and disclosure officers able to identify valuable evidence as it was assessed in real-time
- Allowed for items subject to Legal Professional Privilege to be identified using criteria provided by investigators and sanitised for client review. This material could be made available online separately for independent review if required
- CCL worked with investigators and disclosure officers to ensure the criteria used to identify items forming the basis of the review are recorded, and review progress reports were generated. This ensures that the methodology used to generate final data sets of reviewable material is part of an auditable workflow facilitating compliance with disclosure obligations set out in the Criminal Procedure and Investigations Act (1996) and the Attorney General's Guidelines on Disclosure (2013)

Milestone 3: Online Review

Once a data set responsive to investigative criteria was agreed with the client, this material was prepared and loaded onto the web-based Nuix Web Review environment, which was configured to specific operational requirements. CCL hosted the data in our own secure hosted environment and provided concurrent access to 5 reviewers.

Material released to investigators for review was split into batches according to requirements developed alongside the case team. This was based on:

- Material responsive to a certain group of keywords is reviewed by investigators familiar with the keyword subject area
- Items falling within certain date ranges
- Different file types

During their review, investigators recorded decisions (also known as tags or bookmarks) against all material reviewed. Tags were developed and implemented in line with CCL's recommendations, allowing easy identification of evidential material, unused material, and disclosable material that assists the case of the defence or undermines the prosecution. Comments and disclosure notes were recorded against any reviewed item. This provides the client with a strong case that all necessary disclosure considerations have been taken into account during the first review of material, ensuring no further review of this material is required. The client also utilised the Secured Fields aspect of Nuix to apply further categorisation and comments to items.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Training was delivered to the investigators to ensure they were competent to review the material in the investigation. This training was provided remotely via an online conferencing facility. Ongoing user support time has been provided to the client throughout the duration of the project.

Part way through the investigation, CCL were informed of another government agency that required access to certain exhibits relating to the operation. CCL had to ensure that any LPP considerations on these exhibits were considered again before the data was released to the new agency. It was also imperative to ensure the two-separate review streams (our original client and the new agency) did not interact with each other and the tagging and commenting decisions could not be viewed. As a result, CCL opted to deal with the second enquiry in a different manner. We used the originally processed data within Nuix Workstation and exported out the data required by the new agency to a concordance loadfile format that could be ingested into their own in-house review platform. CCL liaised with their technical team to ensure the format was correct.

As with all cases handled by CCL, exhibit continuity and a chain of custody was maintained for the client's data at all times. All material associated with the operation was treated and handled as Official Sensitive. Using CCL's in-house tracking system, exhibits were tracked to locations at all times and responsive data delivered onsite was encrypted with access only provided to reviewers with individual credentials. Individual logon details to connect to the server and to access the Nuix case files were provided to authorised reviewers. Throughout the acquisition, processing, preparation of data for review and production of the data, Standard Operating Procedures were followed to ensure quality was maintained at all times.

Expertise

Milestone 1: Collection, Processing and Searching
The steps taken to acquire, process and search the data for this operation allowed for the review of a significant amount of data in a proportionate manner. The workflow allows for decisions to be made and recorded whilst utilising the technology available from the Nuix processing engine. The software and workflow suggestions provided to the Contracting Authority will fall in line with those used for this project.

Milestone 2: Searching and Filtering
Potential LPP had to be considered and dealt with as part of the filtering process prior to review. Nuix greatly assists with the steps required to ensure LPP is not released to investigators before Independent assessment. This segregation of data, whether for LPP purposes or purely batching work out to investigators, will be important for the Contracting Authority as outlined in the Appendix 1 requirements.

Milestone 3: Online Review
CCL's proposed solution utilises Nuix Web Review to allow 5 reviewers access to the data. Web Review was hosted by CCL and accessed by the client with secure connection over the internet. CCL have provided a similar implementation suggestion for the Contracting Authority and an alternative method still utilising web review, but within a local environment.

It also illustrates our ability to assist our client in collaborating with other Law Enforcement Agencies

Milestone 4: Production
This project has lasted for a couple of years owing to other commitments from the investigatory team slowing the review. There has also been interaction with another government agency and it was possible to segregate data for them to review. The Contracting Authority may need to keep cases live for a long period of time, Web Review allows you to do so and licences are not tied to a specific project. The case will just sit dormant until required. It is also possible for the Contracting Authority to separate data for review by different parties if required. This may be applicable for review by Independent Counsel or a third-party investigation team.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

A. QUALITY MANAGEMENT

Please provide details of the measures that will be taken to manage and assure the quality of work. You should upload your Quality Assur policy in the supporting documents section of your application.

This should include information on the quality assurance (QA) systems, which have been implemented or are planned, and should be appropriate to the work concerned. All QA systems and procedures should be clear, auditable and may include compliance with internatio

CCL has held ISO17025:2005 accreditation since 2010 for our PC (including Imaging), Sat Nav and Mobile Device laboratori We are accredited to the Forensic Science Regulator's Codes of Practice and Conduct and have transitioned to the new ISO17025:2017.

We hold one of the most comprehensive accreditaiton scopes in the industry. Please see provided schedule of accreditation see our full scope. **(Document 3A – ISO17025 Schedule of Accreditation)**

The standard is maintained by a dedicated Quality team consisting of a Quality Manager, Deputy Quality Manager, Technica Managers and validation specialists embedded in the analytical teams. Analysts and Lab Managers are responsible for the quality of casework.

Standard Operating Procedures: We have a library of Standard Operating Procedures covering the use and operation of a relevant methods, software and equipment, the handling and preparation of items for analysis (including collection, delivery a exhibit receipting procedures), reporting, peer reviewing, purchasing, validation, internal audits, document control, control of records and case data, and dealing with complaints, non-conformances and corrective actions.

Validation: Validation is integral in ensuring the quality of CCL's output. Method validation is undertaken in accordance with Forensic Science Regulator's Codes of Practice and Conduct for the disciplines outlined on CCL's Schedule of Accreditation Validation is carried out by competent validation specialists embedded within the appropriate departments, ensuring the relevancy of the validation. The method validation undertaken not only ensures that the forensic software is suitable for its intended purpose but the overarching examination method is fit for purpose within the confines of the environment in which it implemented.

Validation documentation, including validation plans, test results and validation reports supplemented by software tool refere guides are stored centrally ensuring that analysts have access to the information required during an examination.

Digital forensics is a fast-paced environment and technology is constantly evolving, therefore there are instances when it isn possible to conduct an examination using a validated method. CCL has procedures in place should such a scenario arise, ensuring that the use is risk assessed, authorised, mitigated and communicated accordingly.

Ensuring the Validity of Test Results: CCL has standing operating procedures for ensuring the validity of test results. This includes peer review of every case and participation in proficiency testing which includes set proficiency tests purchased from external test providers, inter-lab testing with other digital forensics organisations and our own case comparisons or intra-lab

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

tests. One of CCL's partners for inter-lab testing is Eurofins, with whom CCL will have a sub-contracting relationship in place this contract. CCL would be happy to undertake inter-lab testing with any Authority using this contract.

Proficiency tests are undertaken in accordance with CCL's Annual Proficiency Testing Plan and results are logged according Any Observations or Non-conformities found within a Proficiency test completed by CCL are handled through our SOP21 - Complaints/Non-Conformance Procedures. This SOP provides details of the procedures for conducting the investigation, remediation and root cause analysis of any issues. The Quality Team regularly reviews all Complaints/Non-Conformances to detect any trends that may have a detrimental effect on casework. If such a trend is found, the Quality Manager produces a report for review by the Management Team.

Peer review involves an experienced colleague who is assessed as appropriately trained and competent in the relevant discipline, checking the Analyst's examination report and generated data. They check the examination has been conducted i accordance with the customer requirements and within the confines of CCL's SOPs. Any comments or suggestions made by reviewer must be responded to by the author and it is mandatory that any issues raised which impact on critical findings are discussed and agreed before the case can be returned to the customer.

Training and Competency: All CCL analysts undergo a programme of training to enable them to acquire and maintain the s and knowledge necessary to conduct forensic analysis of computers and related media and/or mobile devices. This takes th form of an initial induction programme, an assessment of training needs, access to learning resources such as the CCL Wiki, attendance at external or internal training courses (including courtroom skills), shadowing an experienced analyst who is assigned as their mentor and practical assignments, including practice cases.

On successful completion of specific elements of their training schedule, trainees will undertake a competency test. This will involve the analyst conducting a forensic examination on a test case in accordance with the relevant SOPs. This test case w be marked by a senior analyst, technical manager or other designated member of the team.

Following the initial assessment of competency, CCL considers it necessary for all analysts to maintain a high level of competency. The assessment of continued competence is formally tested every two years. This continued competency test assessment will be set and reviewed by the assessor and feedback given to the analyst. The assessment will be based on either a new test case or a thorough and critical review of case(s) recently completed by the analyst. This will be marked usi scoring matrix.

Although all analysts undertake competency testing every two years, their performance is monitored during this period with consideration given to any non-conformances, observations or feedback given by the analyst's peers, mentor, line manager, customers or colleagues.

When new technical methods are formally rolled out that are relevant to the analyst's role during a period of competence, the the individual will receive further training and competency testing appropriate to the new or updated method.

CCL maintains records of relevant authorisations, competence, education and professional qualifications, training, skills and experience and court attendances on our CCL Personnel system. These records are available for inspection.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Continuous Development: In order to maintain our accreditation to ISO17025, ILACG19 and the Forensic Science Regulat Codes of Practice and Conduct, we are audited annually by the United Kingdom Accreditation Service. We have a program whereby we are continually validating new methods and updating previously validated methods and tools in order to broaden scope of accredited digital forensics services.

For example, as our Nuix based solution was being requested more often by our LEA partners it was added to our scope.

New technologies and software are continually reviewed and 'one off' methods are recorded to identify when they become m common and need to be added to the validation roadmap.

As well as obtaining and maintaining our own quality standards CCL have assisted the Forensic Regulator's Team by suppo the writing of Appendices for Method Validation for the Forensics Science Regulator's Codes of Practice and Conduct.

CCL has leveraged our considerable practical experience in gaining and maintaining the standard and offered ISO17025 workshops to Law Enforcement. These workshops emphasised practicalities – how to implement a quality management sys for a digital forensics laboratory and validation of software tools and methods for ISO17025.

In additional CCL holds:

- ISO9001 Quality management systems certification
- ISO27001 Information security certification
- IASME Information Assurance for small to medium enterprises
- Cyber Essentials+ Certification for information security

"It is on CCL's accreditation roadmap to obtain ISO17020 for digital forensics activities conducted on-site. All work carried ou site is undertaken by competent analysts, using methods and tools validated under ISO17025."

B. SUSTAINABILITY

The Food Standards Agency is committed to improving sustainability in the management of operations. Procurement looks to its suppliers to help achieve this goal. You will need to demonstrate your approach to sustainability, in particular how you will apply it to this project taking into account economic, environmental and social aspects. This will be considered as part of our selection process and you must upload your organisations sustainability policies into the eligibility criteria in Bravo.

Please state what (if any) environmental certification you hold or briefly describe your current Environmental Management System (EMS)

Economic

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Providing value for money to the public sector

CCL excels in situations which require abilities over and above commercial off-the-shelf tools. To that end we invest heavily i R&D. Our dedicated R&D team is comprised of individuals who possess strong analytical, research and technical skills. They have extensive experience conducting, supporting and managing investigations. During the life of the contract the team will w closely with our departments to provide insights into new technologies and facilitate the development of new tools and techniques that drive efficiency through the contract. These developments are usually in advance of commercially available solutions.

The focus of CCL is to provide bespoke solutions to assist in investigations. This in turn promotes a significant value propos and affords tactical, strategic and operational benefits, all with no requirement for front end investment from the FSA:

- Access to world class R&D quickly and in line with operational requirements
- Access to significant script library
- The ability to take advantage of specific existing in-house development to reduce cost and risk
- Ability to steer and influence creativity and innovation to enable effective investigation through the life of the contract

Many of our analysts are computer programmers, skilled in languages such as C#, Java, JavaScript and Python. They are al adept at using database management tools (such as SQL and LINQ), regular expressions and various data science techniqu

CCL will work with the FSA to ensure that they maximise the benefit of the contract spend:

- On a case-by-case basis, ensuring that the most efficient investigative workflows are being utilised
- Sharing current and planned innovation that can improve service delivery and efficiency

CCL's Data Analytics team has significant experience of assisting Law Enforcement with developing investigatory workflows ensure the most efficient use of an investigator's time and obtain the best value from the tools at their disposal. This can be d either on an organisational level, benefiting stakeholders across NFCU or in response to the challenges of a specific investigation.

Many of these workflows have been developed to assist with investigations that have LPP requirements and a strong disclos focus due to volumes and complexity of data sources.

Workforce Skills

CCL are committed to working with Universities and Colleges to identify candidates. We offer new graduates a "bootcamp" training and a mentorship programme that upskills and provides workplace experience. In an industry where demand for qua and experienced technical staff is outstripped by demand, CCL is committed to ensuring training opportunities for upskilling technical staff. We have relationships and training programmes with universities that enable graduates to come onto the mar with enhanced skills.

CCL has a Training and Staff Development Policy, the aim of the policy is to

a) Provide induction training for all new employees
b) To provide job specific training to all new and existing employees
c) To identify the longer-term development needs of employees

We already have a number of support staff who have taken advantage of apprenticeship opportunities. We are committed to continuing our apprenticeship programme.

Benchmarking performance and identifying areas for improvement

CCL can implement a number of mechanisms for benchmarking performance including:

- Regular management reporting against KPIs

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- Reporting on innovation and added value
- Obtaining feedback from clients and ensuring that it is fed back into a cycle of continuous improvement forms part of CCL's ISO17025 accreditation, this will take the form of:
- Obtaining feedback from individual investigators at the conclusion of a case (via surveys)
- Regular contract meetings
- Collating unsolicited feedback
- Ensuring that analysts and R&D team members share best practice internally

Environmental

"Proper regard for environmental issues while still securing value for money"

Protection of the environment is important to us and is part of our values and principles and we consider it to be sound busin practice. Care for the environment is one of our key responsibilities and an important part of the way in which we do busines order to protect the environment, we commit our company to maintain and implement an environmental policy. CCL's Qualit Manager and Compliance Manager is responsible for the maintenance and implementation of our environment policy which been provided.

Social

Stakeholder Benefits

CCL Group are led by CEO Noel McMenamin, former Head of the West Midlands Regional Organised Crime Unit, who work under the stewardship of Chairman and former Head of the National Crime Agency, Keith Bristow. Their values, leadership s and interest in the criminal justice system have been carried into their work in the private sector. This has created a philosop CCL that offers benefits and value for money to officers, the public and the Criminal Justice System.

Equal Opportunities

CCL is committed to promoting equality of opportunity for all employees and job applicants. It aims to create a working environment in which all individuals are able to make best use of their skills, free from discrimination or harassment and in w all decisions are based on merit.

CCL's Equal Opportunities policy (provided) forms part of our Employee Handbook, which is part of our employee's contract.

The Company is committed to promoting equality of opportunity for all employees and job applicants. It aims to create a wo environment in which all individuals are able to make best use of their skills, free from discrimination or harassment, and in w all decisions are based on merit.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

The Company does not discriminate on the basis of gender, sexual orientation, marital or civil partner status, gender reassign race, colour, nationality, ethnic or national origin, religion or belief, pregnancy or maternity, disability or age (the prote characteristics).

The principles of non-discrimination and equality of opportunity also apply to the way in which employees treat visitors, cli customers, suppliers and former employees.

All employees have a duty to act in accordance with this policy and treat colleagues with dignity at all times, and not to discrim against or harass other employees, regardless of their status.

To ensure that the policy operates in practice for all staff, including staff working on the HMRC contract, CCL maintains and re the employment records of all employees. Monitoring may involve:

a) The collection and classification of information regarding the race in terms of ethnic/national origin and sex of all applic and current employees;
b) The examination by ethnic/national origin and sex of the distribution of employees and the success rate of the applic and
c) Recording recruitment, training and promotional records of all employees, the decisions reached and the reason for t decisions.

This data can be provided, subject to data protection legislation.

Community Relations

CCL Group are actively engaged in the community by supporting both local and national charities. In just the last year, we ha raised £2500 for NSPCC via a team of skydivers, sponsored Safeline's 25th anniversary drinks and raised £1,000 for The Shakespeare Hospice by participating in a Dragon Boat Race. We also donated all of our old computers to IT Schools Africa provide e-learning technology to students and local communities in Africa. Additionally, we've raised a further £500 for variou charities via internal events. These charities are selected by staff and are often very close to employees' hearts. This encouragement of charitable giving not only increases visibility within the community for both the business and the charity bu also provides fun and engagement within the office which in turn boosts morale.

CCL is a member of the West Midlands Chamber of Commerce.

C. ETHICS

Please identify the key ethical issues for this project and how these will be managed. Please respond to any issues raised in the Specificat document

Please describe the ethical issues of any involvement of people, human samples, animal research or personal data in this part. In addition please describe the ethical review and governance arrangements that would apply to the work done.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Applicants are reminded that, where appropriate, the need to obtain clearance for the proposed project from their local ethics committee. is the responsibility of the project Lead Applicant. However, if a sub-contractor requires such clearance the project Lead Applicant should ensure that all relevant procedures have been followed. If there are no ethical issues please state this

A number of the ethical considerations related above (human samples, animal research) are not relevant to this contract.

The ethical considerations that are relevant are related to CCL's duty the court. This being that the primary duty of an expert witness is to the court. This overrides any obligation to the paying or instructing party.

CCL's training ensures that all our staff are aware of their obligations in relation to the appropriate statutes and practice directions. Our peer review of cases takes these into account when assessing a completed case.

D. DATA PROTECTION

Please identify any specific data protection issues for this project and how these will be managed. Please respond to any specific issues ra in the Specification document.

Please note that the successful Applicant will be expected to comply with the Data Protection Act (DPA) 1998 and ensure that any informa collected, processed and transferred on behalf of the FSA, will be held and transferred securely.

In this part please provide details of the practices and systems which are in place for handling data securely including transmission betwee the field and head office and then to the FSA. Plans for how data will be deposited (i.e. within a community or institutional database/archiv and/or procedures for the destruction of physical and system data should also be included in this part (this is particularly relevant for surve data and personal data collected from clinical research trials). The project Lead Applicant will be responsible for ensuring that they and ar sub-contractor who processes or handles information on behalf of the FSA are conducted securely.

Data protection policies

CCL holds the following certifications: ISO27001, Cyber Essentials Plus and IASME Gold.

The standards were achieved and are maintained by CCL's Quality & Compliance Manager, IT Support Team and Quality T An information security management system is maintained, built on the principles of ISO27001 and incorporating the other standards. In order to obtain and maintain CCL:

- Systematically examined our information security risks, taking account of the threats, vulnerabilities, and impacts
- Designed and implemented a coherent and comprehensive suite of information security controls to address those ris
- Adopted an overarching management process to ensure that the information security controls continue to meet information security needs on an ongoing basis. The strategy takes note of the following areas:
  - Senior management strong support of information security initiatives
  - Milestones and timelines are set for all aspects of information security management to help ensure future succes and continual improvement of the system

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Card issued to staff. The exhibits are tracked to an individual during their interaction and tracked out of the business when th leave.

E. PROJECT MANAGEMENT

Please fully describe how the project will be managed to ensure that objectives and deliverables will be achieved on time and on budget. Please describe how different organisations/staff will interact to deliver the desired outcomes.

Highlight any in-house or external accreditation for the project management system and how this relates to this project.

Methodology for managing individual projects is detailed in our response to the scenario questions. This refers to our management of the contract as a whole.

CCL has considerable experience of managing contracts of this nature including operating major contracts with NCA (contract also includes providing services to Home Office Immigration enforcement and Greater Manchester Police), HMRC, Mass (Metropolitan Police Service), West Yorkshire Police and West Midlands Police.

CCL will provide a dedicated Contract Management Team, consisting of:

- Contract Sponsor (Senior Responsible Owner & Commercial Director) - a member of CCL's Executive management team responsible for ensuring that proper resource is dedicated at a corporate level and that servicing the contract forms part of company strategy. HMRC's ultimate point of escalation.
- Account Manager (Commercial and Mobilisation Manager) – overall responsibility for the contract, HMRC's initial point of escalation
- Forensic Case Team – Nominated members of CCL's dedicated Forensic Case Team will be responsible for: Day-to-day communications with client and officers
  - Managing submissions (including collection/delivery)
  - Managing TRTs
  - Providing updates on case progress
  - Providing required management information
  - Managing requests for additional work
- Data Analytics Support Technician – Responsible for requests and support relating to use of the online review platform
- Finance Team - Assisting in the production of management information and invoices
- Quality Manager – Dealing with feedback/complaints, requirements around quality standards (e.g. arranging inter-lab testing)
- Functional Technical Leads – A nominated technical manager in each area (Mobile Device Analysis, PC Analysis, Data Analytics)

To ensure CCL meets the specific requirements of the client, particularly with regard to deliverables CCL offer specific and dedicated work instructions. CCL will write a work instruction which serves to document the specific requirements of the FSA. Analysts use the work instruction when conducting their examinations.

Time, budget and change control

Each analyst belongs to a team with a Team Manager who actively ensures that cases are managed properly and analysts have the necessary resources to investigate properly.

Prime responsibility for ensuring timescales are met belongs to the analyst and Team Manager, but CCL also manages cases corporately by maintaining electronic records within a case management system. Regular Operations Meetings ensure that potential resourcing issues are recognised early and mitigated.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

The analyst is required to maintain contact with the client to ensure that the objectives of the case are properly considered, that any issues are promptly raised and addressed, and timescales are monitored. Where multiple disciplines are required to complete a case a lead analyst is assigned.

It is possible that as a case progresses, new factors will emerge. These factors may require more time than originally estimated. As soon as the scope of the enquiry changes or the analyst becomes aware that the case will require more time than originally estimated, they will discuss this with the client. With new lines of enquiry, this will involve weighing time constraints against the value of any additional evidence sought. Where the issue is the volume of the evidence found, the analyst will agree a strategy that achieves the evidential objectives in the timeliest and most cost-effective way. No additional work is undertaken without appropriate customer approval.

Technology Solutions

CCL is continually researching emergent technologies that can assist in efficient and effective delivery of our services. Our management and operations team engage with industry leading software vendors to ensure they are sighted on any new updates to functionality that would benefit CCL and our customers.

CCL's ISO1025 method and software implementation including process, software and hardware provides visibility of any limitations or areas of improvement. Any software and technologies identified for improvement are added on our roadmap for review and possible implementation.

4: THE SCENARIO – DETAILS RELATING SPECFICALLY TO THE SCENERIO

A. Approach/SCOPE OF WORK

Please describe how you will meet our specification in relation to the given scenario. how you will deliver your solution. You must explain the approach for the proposed work. Describe and justify the approach, methodology and study design, where applicable, that will be used to address the specific requirements.

CCL can provide all aspects of Digital Forensic ("DF") services required for the described scenario ("the Scenario") in support of a NFCU food crime investigation. For CCL this process starts with gaining a full understanding of client needs, recognising that no two investigations have identical DF objectives and requirements. The CCL approach to the Scenario can meet and exceed NFCU deliverables, whilst operating to our ISO17025 standard operating procedures.

Whilst evidential products are the principle deliverable in an engagement, CCL fully understand the importance of complying with disclosure obligations in civil and criminal casework. CCL standard procedures include contemporaneous note-taking throughout all examinations (whether at a scene or in the laboratory) and the compilation of a disclosure schedule for return with evidence and case archive material. The CCL Data Analytics Team ("the DA Team") have expertise in assisting complex Law Enforcement investigations where the management of data and associated disclosure obligations have presented an obstacle to an otherwise successful prosecution. In complex casework CCL assists its clients with the formulation of a bespoke Programme of Work framed within the parameters of an Investigation Strategy ("the Strategy") and associated Disclosure Management Document ("the DMD"). Whilst the Strategy and DMD are the remit of a client, CCL is well placed to advise on the formulation of both in the context of technology and legal landscapes with expert internal staff knowledge and/or assistance from a partner law firm where required.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Adherence to specific ISO17025 approved CCL processes and procedures guarantee CCL examiners deliver accurate, and reliable evidence. All CCL statements and reports outline the expertise of the author in terms of their qualifications, certifications and industry experience. CCL basic employment requirements typically include a relevant undergraduate degree, many examiners also hold postgraduate qualifications. New starters at CCL undergo rigorous training and competency testing before being adjudged to be proficient to conduct casework. CCL examiners regularly attend Crown Court to present live evidence across the UK in a professional or expert witness capacity.

CCL laboratory examinations occur within the framework of CCL's ISO accreditation scope which covers computer and memory imaging, mobile device extraction and analysis processing to provide support online remote review examination. The CCL ISO accreditation also covers validated methods using forensic tools including Axiom, EnCase, Nuix and X-Ways. Where an examination requires out of scope techniques or tools prior written client permission is always obtained.

Each client is assigned a dedicated CCL Forensic Case Team ("FCT") contact who manages all aspects of exhibit submission, retention and return. In addition, a named member of each laboratory team co-ordinates their respective activities and dependant on the case type an overall internal CCL lead for a multidisciplinary case is appointed. This person is responsible for maintaining contact with the lead client case investigator and will update to confirm tasks such as completion of imaging, triage, processing, review readiness and evidence production. The list is not exhaustive and regular communication between the client and CCL lead is expected on regular basis as the case progresses. CCL provide email, landline and mobile contact details at the commencement of an engagement to assure effective and accessible client communication. In the Scenario the CCL case team lead would be a Consultant or Project Manager on the DA Team.

At the commencement of an engagement and with sight of an associated NFCU supplied work package, CCL will conduct a scoping call with the NFCU to confirm specific needs, objectives and linked deliverable requirements. In response to the engagement request CCL will provide an estimate quote outlining a Programme of Work, ("the PoW") deliverable outcomes, pricing and approval mechanisms which CCL believe are necessary to deliver the supplied NFCU Work Package. Should CCL be engaged by NFCU to deliver a work package then detailed planning and preparation will commence with the assistance of NFCU.

A PoW has been provided for this scenario and is included as document 4A – Programme of Work.

CCL aims to fulfil the role of a dependable partner in an engagement by providing a quality service from an independent and knowledgeable perspective whether that is in support of internal NFCU DF resources or as compliment to them. The service provided by CCL's laboratories extends traditional DF laboratory data in/data out workflow patterns by iteratively working with clients throughout an engagement to check requirements and improve outcomes. This approach can be extended to meet the NFCU requirement for update and understanding on emerging technologies. CCL's dedicated Research and Development Team can provide ad-hoc or regular training and information to explain emerging technologies and their technical DF solutions. CCL's DA Team are similarly well placed to advise on Cloud collections and the latest assisted review technology developments.

The tender scenario provides an excellent opportunity for CCL to detail the processes and outcomes of an engagement and is addresses in detail in the following paragraphs and by an appended sample quote and linked DF Investigation Strategy. The quote details the PoW in terms of deliverables, a timeframe and cost estimates. Some elements of an

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

engagement will always remain unknown before commencement of enforcement activities but can often be estimated. These elements include review data volumes, reporting requirements and court appearance likelihood. CCL has detailed experience and provides estimates on a best-case scenario for the anticipated length of time and resource required to conduct each deliverable activity. Where unexpected or additional requirements are encountered over and above an original estimate CCL always seek prior written client authority for additional work to be conducted.

Please provide details of any aspect of the proposed work which are considered innovative in design and/or application? E.g. Introduction of new or significant improved products, services, methods, processes, markets and forms of organization

.

SPEKTOR Triage Tool

During the onsite phase of the project CCL may utilize our SPEKTOR tool, this allows us to:

- Make an informed decision about the digital forensic evidential yield across a range of devices on site.
- Provide efficiencies, it helps to reduce costs by reducing the number of seized items that require fuller examination.
- Provide early evidence for interview and increase the opportunity to obtain early guilty pleas, saving on lengthy prosecution costs.

Some of the Technical advantages of using SPEKTOR to triage devices are:

- SPEKTOR is very fast at triage of data due to its powerful prioritisation engine which quickly identifies files of interest based on user-specified criteria and collects from the target media for later analysis by SPEKTOR or performs 'Direct Analysis', showing real-time results during the collection process.
- Performs full-speed interactive review during the processing stage without a pause in processing.
- SPEKTOR images very rapidly. A typical 1TB mechanical disk in a laptop is completed in 1h20m and a 500Gb SSD imaged at speeds in excess of 200GB/m (both via USB3).
- SPEKTOR Ultra performs even faster by imaging MULTIPLE devices simultaneously at speed. i.e. 4 x USB sticks (total 128Gb) imaged in 4.5 minutes.
- Ability to use almost unlimited keyword lists. Supports searching in multiple languages.
- Ability to use more than 100M hash values as both Watch Lists and Ignore Lists.
- Automatically attempts dictionary attacks against password protected files.
- Ability to perform triage on existing forensic images.
- Automatically finds geolocation data, credit card numbers, digital currency addresses, etc.
- Flexible enough for any type of investigation. Fraud, e-discovery, IP theft and system misuse are easily examined.
- Analyses data from the latest Internet Explorer and MS Edge technologies.
- Supports PC, MAC and Linux systems.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- Analysis of iPhone backups. Dual Boot option allows any Windows tools to be installed such as MOBILedit, Encase etc.
- Reconstructs web pages from the browser cache giving a view of what the user saw.
- The tool is Linux-based but requires no knowledge of Linux. Unlike Windows-based systems, it does not leave potentially compromising evidence or intelligence on the host system's hard disk.

Workflow Consultancy

CCL's Data Analytics team has significant experience of assisting Law Enforcement with developing investigatory workflows that ensure the most efficient use of an investigator's time and obtain the best value from the tools at their disposal. This process adheres to best practice but ensures that the workflows are uniquely adapted to meet the challenges of an individual case. These workflows offer significantly improve usage of existing commercial review platforms.

R&D Team

CCL excels in situations which require abilities over and above commercial off-the-shelf tools. To that end we invest heavily in R&D. Our dedicated R&D team is comprised of individuals who possess strong analytical, research and technical skills. They have extensive experience conducting, supporting and managing investigations.

The focus of CCL is to provide bespoke solutions to assist in investigations. This in turn promotes a significant value proposition and affords tactical, strategic and operational benefits.

- Access to world class R&D quickly and in line with operational requirements
- Access to significant script library

Many of our analysts are computer programmers, skilled in languages such as C#, Java, JavaScript and Python. They are also adept at using database management tools (such as SQL and LINQ), regular expressions and various data science techniques.

THE SCENARIO - PLAN AND DELIVERABLES

A. The Plan

Please provide a detailed project plan including, the tasks and sub-tasks required for the scenario.

Below is a detailed description of the project phases. Please see document 4A Gannt Chart for Project Plan

Investigation Planning – Identification/Preservation

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

The Scenario requires CCL assistance and engagement to assist NFCU conduct a co-ordinated enforcement action at three separate business premises. One premise is an office and the other two are industrial food production factories. On engagement CCL/NFCU would schedule an exploratory scoping call to check the requirements of the provided NFCU Work Package. Issues to be discussed and associated CCL capabilities would include:

1) Detailing a list of the services required to meet the Work Package, including; scene examinations, lab imaging, data processing and analysis, remote review, evidence production and presentation.
2) The Scenario also includes a specific requirement for data transformation and potential reverse engineering of labelling record log formats to enable correlation of historical labelling records with their industrial labelling machine outputs. CCL's Research and Development Teams are well placed to assist with this type of work and have the capability to conduct advanced and effective liaison with a label machine manufacturer in order to determine the best options for examination at the factory scenes, thereafter to provide log data in a format enabling the manufacturer to provide NFCU with expert evidence. This work would be conducted within the parameters of CCL processes and procedures to deliver an evidential product whose continuity is assured and accurately described.
3) A requirement for scene attendance within a 48-hour time frame is noted in the Scenario and would be confirmed. CCL are used to assisting private and public sector clients with data collections within very tight timeframes, often assisting clients with an urgent requirement to collect data from the UK and abroad from personal computers, servers, mobile phones and storage devices of all types. To facilitate this work, CCL, maintain an on-call system of available analysts, supported by dedicated, checked and sealed response equipment and vehicles at their offices in Stratford-Upon-Avon. CCL can typically reach all major conurbations in England and Wales in under four hours and are used to attending scenes to conduct examinations with little notice outside of ordinary working hours.
4) If appropriate CCL would expect to attend a pre enforcement briefing online in order to check equipment requirements and understand any intelligence relevant to scene examination activities. CCL would also expect to attend the enforcement day briefing in person provided prior to scene attendance requirement in order to check legal authorities, understand specific safety and examination details and provide relevant advice to the NFCU if required. CCL examiners are all HM Government Security Vetted (SC level) and understand the need to know principles of intelligence handling.
5) Details of safety measures in place to protect CCL staff at factory and office premises would be confirmed. CCL have specific procedures in place for dealing with bio-hazardous material and understand the requirement to be guided by NFCU in an industrial setting in terms of wearing supplied personal protective equipment and following specific safety advice.
6) Mindful of business continuity, the national nature of the Scenario company and its role in the food supply chain, CCL would seek to establish if as a first option data required from servers could be imaged live and as a second option whether the graceful shutdown of servers and storage could be accomplished followed by rapid imaging and (if required) return of original equipment to the Scenario business.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

7) As many businesses now store their email, loose files and web application data remotely CCL would seek to establish if legal authority or consent would allow the collection of remotely stored data and plan accordingly.
8) CCL note in the Scenario that files to be reviewed are typically office productivity types and that there may be other aspects to the offences being investigated which suggest financial gain and associated record keeping. Often financial and accounting records are stored in proprietary formats. CCL would seek to establish any additional requirement to collect, analyse and report on this type of record, e.g. the Scenario mentioned Chorus accounting data and backups.
9) CCL would provide a summary of the scoping call, any action points, contact details for the FCT, other team leads, and biographies of staff dedicated to the various Work Package tasks following the scoping call
10) In accordance with NFCU requirements CCL would contribute and help determine the Digital Forensic Strategy for this deployment/ operation.

Collection

After attending the enforcement action briefing and in accordance with the Forensic Strategy, CCL staff, typically two per venue, would attend scenes with NFCU, entering when safe to do so. Guided by NFCU, CCL staff would triage devices and offer consultancy on seizure and Laboratory examination. CCL staff would engage in a step by step process for each exhibit to assist NFCU safely secure evidence and storage of seized items. This process can be described in terms:

1) Checking availability of power supply, e.g. are laptop computers being charged.
2) An assessment of whether disconnection of networked devices from the internet is required to prevent remote wiping instructions being issued and communications being delivered after seizure of a device.
3) If available and trusted, (by remote call or onsite interaction) a conversation with local Network Administrator(s) to determine network extent and configuration.
4) Establishing network connectivity and powered on computer IP Addresses and MAC identifiers, by a combination of live examination and/or examination of network switches, routers and server settings. This may be particularly relevant for the Scenario labelling machines to enable correlation of specific machines with their remotely stored logs.
5) If required, the live capture of volatile memory from powered on computers and laptops.
6) Collection of access passwords and passcodes for devices whose data may be encrypted at rest. This point being particularly important for the examination of mobile devices or encrypted computers which may be inaccessible for examination without passcode access.
7) Consideration for vulnerable data stored at rest on devices; e.g. Recently Deleted files, message retention and system clock settings
8) A consultation with network administrators and business managers to establish the likely impact on food production or factory safety if computers and machines are turned off or temporarily removed from the network.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

The explanation of any such factor to NFCU staff for the implementation of any decision to image in place or seize.

9) In the Scenario provided it appears that a decision has been made to order disconnection and graceful shutdown of all equipment for remote laboratory examination and the rest of this scenario planning is described on that basis. CCL have proprietary technology available which would enable rapid triaged imaging of data from computers and storage media and extraction of mobile devices at scene, as an alternative to seizure if required and would attend any scene in possession of this technology solution in any event.
10) Examination of the Labelling Machines (effectively an Industrial Control System) could include copying any operating system disc, noting connectivity and establishing IP Addresses for each machine. It may also be possible to establish the path for any data historians (the NAS backups perhaps) via live examination and conduct a live limited test label run to establish the accuracy and content of logged data as it relates to produced labels.
11) During all live examination processes CCL staff would make contemporaneous notes, including photographic records.
12) After any initial live imaging, assessment of encryption and networking examinations were completed CCL staff would assure that each powered-on computer to be seized was gracefully shutdown in order to preserve its operating state and future capability for laboratory examination and return use. This could include placing a laptop in hibernation mode to preserve otherwise uncollected volatile memory. On successful shutdown of a computer and physical disconnection from the network CCL staff would hand responsibility for the item to an NFCU investigator for seizure and appropriate packaging.
13) On completion of packaging tasks by NFCU, CCL's secure exhibit delivery service (a custom, secure van driven by a security vetted member of staff) would take receipt of any exhibits to be transported to CCL Laboratories, noting exhibit descriptions and bag seal references.
14) On arrival at CCL Laboratories a member of the Forensic Case Team would take receipt of exhibits seized, noting descriptions and the integrity of exhibits bags and their seal references. The same member of CCL staff would log the exhibits against a case reference on CCL's exhibit handling and case management systems before placing them in CCL's UK Government grade approved secure storage facilities. The secure store is access controlled and like CCL offices is subject to continuous video recording.

Imaging and Extraction

1) In the Scenario described devices seized or examined fall into five distinct categories; mobile phones, personal computers, server computers, network attached storage archives and industrial control systems (i.e. labelling machines).

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

2) Any data retrieved by an examiner or device seized at the scene would be retrieved from the secure store and audit logs completed showing temporary transfer out of the store.
3) Mobile phones would be examined by the Mobile Device Laboratory to obtain the best possible extraction of data, with any exceptions being noted. An examination report for each device using the most appropriate forensic tool would be forwarded to the NFCU for consideration of potentially missing items and the application of non-standard, advanced or out of scope methods to recover further data. This could be a further requirement for passcodes, physical device repair or use of an advanced extraction method. On completion of the examination the Analyst would prepare a package of evidence (typically in Cellebrite UFDR format) suitable for ingestion to Nuix Workstation software. The evidence package being archived to a compressed format and copied using an internal CCL secure copy tool (Paranoid Copier) to a data store which the DA Team have access to with copies of the transfer logs confirming data continuity. Mobile Device Analysts would prepare a statement for each device examined at the time of examination. The mobile phones in the scenario are all capable of being examined by CCL with appropriate access codes supplied where necessary. Individual considerations for the phone types are:
    a. Samsung Galaxy S10 Mobile phones
        i. Operating system: Android
        ii. Accessibility: yes. Passcode provided
        iii. Operating system version?
        iv. Device firmware version?
        v. Extraction support on commercial tool: Advanced logical by UFED
    b. iPhone XS mobile phone
        i. Operating system: iOS
        ii. Accessibility: yes. Passcode provided
        iii. Extraction support on commercial tool: Advanced logical by CheckRa1n
4) Analysts would be aware of the below vulnerable data settings for both smartphone platforms adjusting the setting or conducting extractions immediately to avoid loss of evidence.
5) Analysts would be aware of the below Android settings:
    a. Secure start-up or secure/hidden folders enabled
    b. Recently Deleted media files
    c. Notes application Recently Deleted
6) Analysts would be aware of the below iOS settings:
    a. Recently Deleted media files
    b. Keep Messages
    c. Voice memo (clear deleted)
    d. Notes application Recently Deleted
    e. Remove Deleted Emails
7) Recovered evidence would be verified in accordance with the case strategy to ensure volume and accuracy of data was correct.
8) Upon successful verification of the extracted data, the Analyst would include said data in their UFDR or XRY Reader output.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

9) If extracted data relevant to the examination strategy did not extract accurately, the Analyst would consider the use of other tools and techniques. If potentially relevant to the investigation, the Analyst would raise the limitation of the tool in their examination report for the client to assess proportionality of additional work. No additional work would be conducted without prior authority from the client.
10) The Mobile Device Laboratory also has expertise in the examination of Sat-Nav devices and other non-routine mobile devices such as drones and tracking devices.
11) Personal computers (the four Lenovo Think Pad T480 laptops, one MacBook Pro laptop and three iMac personal computers), would be examined by CCL's imaging technicians and the created forensic images replicated. Using write blockers where possible the forensic imaging team would also create bit for bit copies of any data captured at the various scenes with full continuity and contemporaneous notes and completing imaging statements post collection.
12) It is of note that the iMac computers contain 1TB SSD hard drives as CCL's previously mentioned SPEKTOR Rapid imaging technology could be used at the scene to rapidly forensically image these devices, typically under one-hour thirty minutes for each. The same technology could be used to rapidly image the Mac and PC laptops conventional hard drives although this would take a little longer depending on the disk speed and contents. By way of example:
    a. A full image of a 128GB SSD in a MacBook Air (non T2) (60% full) took under five minutes versus fifty-five minutes using standard tools
    b. A full image of a 1TB mechanical HDD (75% full) in a Lenovo ThinkPad took under one-hour twenty minutes including verification more than five hours using standard tools.
    c. Should the MacBook Pro have T2 encryption the latest version of MacQuisition will be used to acquire a full bit for bit copy. Username and password information will be required and obtained to ensure a full and complete copy is acquired
13) It is also worthy of mention that although not referenced in the Scenario many businesses routinely encrypt their data at rest on computers and laptops to assure data security and compliance with GDPR obligations. CCL's imaging technicians are well versed in checking for such encryption in copied forensic images and subsequently obtaining a decrypted copy of an encrypted forensic image for supply to the DA Team.
14) The two NAS backups, six servers, two from HQ premises and two each from the factory premises would be a priority to image and return to NFCU. CCL's imaging laboratory often works extended hours to provide this type of imaging requirement and with notice would be aiming for a maximum 48hr turnaround from first receipt at the laboratory. Servers and NAS devices would reasonably be expected to use a Redundant Array of Disks ("RAID"). The options for imaging a device containing a RAID include creating an image each disk and then rebuild the created images in the RAID to a single logical volume, thereafter, capturing a forensic image of the RAID content. Whilst CCL has great expertise in forensically rebuilding RAID volumes, the approach is not always successful. CCL would therefore recommend taking a forensic image of each disk in a server as a backup for the original. With original discs replaced CCL imaging technicians would then perform a forensic boot of each server using an ISO17025 accredited Linux operating system and using its inbuilt forensic imaging tools seek to obtain a forensic image of the server RAID.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

15) Similar considerations would apply to the NAS storage devices which often may only be able to be acquired as a read only mounted volume due to the proprietary nature of their hardware and software.
16) The imaging team would transfer copies of the complete, iMac, Laptop, Server and NAS RAID forensic images to Data Analytics Team storage, using Paranoid Copier and providing logs.
17) The Imaging Team would also make the NAS backup (believed to contain labelling machine logs) available to the CCL Research and Development Team along with copies of any extractions, photographs or network connection details relating to examination of the labelling machines at the scene for further analysis and supply of machine distributor accessible data to the NFCU.
18) Additionally, the Imaging Team would make the Chorus accounting backup available to the Research and Development Team for assessment as to access and conversion to accounts data accessible to the NFCU or their agent. CCL have internal capability and expertise in Audit and Accounting software and work with external specialist partners to deliver bespoke specialist examination of accounting data with detailed reporting if required.
19) The result of all collection and imaging work would be a defined data set, whose integrity can be demonstrated, provided to the DA Team for further processing, analysis and review provision.

Processing

1) On confirmed receipt of all data sources the DA Team would check the forensic integrity of all data provided by the phone lab and commence an ISO17025 accredited method of processing the data using Nuix Forensic Workstation software.
2) The process may include assigning a nominal data custodian to each data source, e.g. the names of directors linked to various phone and laptop exhibits.
3) Nuix Workstation can process and index many file system types including Windows, Linux, iOS and OSX file systems from forensic images and mobile phone extractions.
4) For complex investigations the DA Team typically process data in distinct phases to identify and index the data types relevant to an investigation review. For the described scenario this is likely to be office productivity documents and communications including email and messaging of various types.
5) Nuix is capable of processing images and non-searchable documents to identify text using Optical Character Recognition (“OCR”) software. This activity is performed as a standard part of CCL processing.
6) Once all processing and OCR is complete and quality assurance checks conducted to assure all encrypted files and containers are identified and other files are processed as expected (with exceptions examined and separately analysed/converted to a processable format as necessary) a collection of simple Nuix cases would be compounded to a single Nuix case. A Compound Nuix case enables case wider searching and further analysis.

Analysis

1) The scenario describes the NFCU supply of a Word List to identify potentially relevant review data. In an automated process the DA Team can search across lists of many hundreds of search terms to identify responsive results in processed data in a few seconds or minutes.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

2) Searches can be run across all file or communication content and metadata (information about the file, e.g. email sender or document author).
3) Typically, CCL works with clients in an iterative process to determine a list of search terms (or parameter such as dates or email domains/addresses) which strike a balance between investigation requirements and review capability. Once the client is satisfied with scope search results the searches are run to bookmark (tag) search responsive files for provision in review.
4) CCL can also assist with the development of other robust review techniques designed to quickly identify evidence whilst maintaining a commitment to pursuing investigative lines of enquiry and disclosure obligations. Alternative approaches to a linear review based on key word searches can be combined and include:
    a. A review of files and communications based on value parameters, e.g. date ranges, types of communication, specified email mailboxes or file types.
    b. A first pass search and linear review of files and communications identified by reference to entities connected with an investigation (e.g. phone numbers, messaging names, email addresses, names, passport numbers, account numbers and company names). A secondary linear review of all evidential items connected with first pass items by communication thread, file location or other factor, followed by a third review of all other items responsive to key terms established by reference to relevant content in the first two reviews. In this type of review the connectivity of evidence associated with investigation subjects is established at an early stage and compilation of an active case summary can be completed in tandem with conduct of the review.
    c. Technology assisted review to identify concepts in data, clustering similar results together by topic (concept search).
    d. Technology assisted review to identify a subset of case data likely to be relevant based on a small quality assured randomly selected review sample (predictive coding (TAR)).
    e. Technology assisted review to identify items of high similarity to those already selected as of relevance to one or more case issues on an ongoing basis (continuous active learning (TAR2)).
5) CCL often find that greater efficiency in review can be achieved by further analysis and although not required in the Scenario would recommend that de-duplication of loose file data by reference to its unique algorithmically created value (hash) and deduplication of emails by their conversation thread identifiers is conducted (to identify a minimum corpus of top level chain emails and their various in chain attachments) prior to searching of data. Deduplication of these types can be conducted on a whole case or per custodian basis.

Review

1) Although not also mentioned specifically in the Scenario (but referenced elsewhere) a search of the Nuix Compound Case data for files whose content could be subject to Legal Professional Privilege (“LPP”) is often

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

required prior to the commencement of a review. The process of providing a review where LPP is also a consideration is described for completeness.

2) CCL have many years of experience in assisting Corporate and Law Enforcement partners identify, segregate and handle sensitive and privileged material. Standard forensic methods may not provide the necessary control and flexibility to deal with material subject to LPP, due to the stringent way in which documents must be handled without introducing significant delays or costs. CCL have developed specific workflows utilising Nuix to process all data in a case, identify, segregate and provide data with potential LPP content to independent Counsel for review. CCL would typically employ the following processes:
    a. All acquired data is processed to make it searchable.
    b. LPP searches are conducted across the whole case, a subset of exhibits or across the subset of data identified for review by key search term. If properly managed within the parameters of a well written DMD the later approach which excludes all other data from review can be very cost effective as it effectively segregates part of the investigation material which in case terms is not examined to discover evidence.
    c. An LPP keyword search is executed over the selected data set thought to contain LPP relevant file types. A report listing keywords executed and the number of items responsive to each keyword is provided to a Client or their Counsel to assess whether the volume of data is proportionate to conduct further review.
    d. LPP data is exported into a separate Nuix case file for review by independent Counsel who conduct a deterministic review to establish whether each file or communication contains LPP content. Counsel can also apply free-text comments which may assist with scheduling items for disclosure. In all cases, access to LPP data is only provided to authorised individuals via their own named user accounts.
    e. In parallel to the LPP review, non-LPP data is exported into a separate Nuix case file for remote review by the case team. Under no circumstances will the case team have access to material being assessed by Counsel. CCL have quality assurance checks in place to ensure that prior to the release of data to a reviewer, the setup configuration and case access is peer-checked and documented.
    f. Following independent Counsel review, material assessed by counsel as NOT privileged will be released back to the case team for review, whilst material assessed as privileged will remain excluded from the case team review.
    g. For items which are part privileged it is possible to allow a redacted PDF version of the original file or communication with any LPP content masked to be viewed by the case team.
    h. To ensure the case team does not have access to any LPP material, the data is provided to them for review without providing access to the forensic acquisitions (as these would contain all data extracted from the exhibits).
3) Our experience in dealing with LPP cases has highlighted the importance of the relationship's documents hold, for example emails and attachments, when isolating data. When keyword searches are used to separate potential LPP, items in the same family should be kept together and when one item is potentially LPP, all family items are reviewed by independent Counsel prior to release to the case team. Nuix allows for subset cases to be created that takes data responsive to keywords and their family items and does not allow viewing for the rest of the data within the main dataset. This allows for the clean separation of data and provides different casefiles for independent Counsel and Case Officers to work from.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

4) CCL are happy to share our workflows and experience should NFCU require. CCL have assisted Law Enforcement agencies on many occasions with LPP cases, many of which have resulted in successful prosecutions.
5) Throughout a review the lead DA Team examiner will liaise with the NCFU lead investigator to ascertain and resolve any issues relating to files which cannot be easily viewed.
6) Reference is made above to using Nuix review software (currently named 'Nuix Investigate'), however once data has been successfully processed using Nuix Forensic Workstation software a variety of options are available for conducting remote review. Each review software has at its core an ability to provide controlled and secure access to review data remotely via web browser access.
7) Exported review data can be viewed via the Nuix Investigate platform which has, as its name suggests, Investigation as a core use case. The software has many features to assist a reviewer following an investigation strategy identify useful information and evidence quickly. Data could also be made available via the 'Nuix Discover' review platform or the 'Relativity One' review platform. Each of these alternative software has comprehensive analytical features for technology assisted review and an inbuilt ability to provide court ready documentation. Data identified as evidence in Nuix Investigate can be easily loaded to either platform for legal review which is their intended use case. For the purpose of the scenario review the use of Nuix Investigate alone is described.
8) Following the preparation of the data, CCL's analysts will manage the processing and quality assurance of data throughout the processing stage and will prepare the data so that it is remotely accessible by NFCU for review.
9) Nuix Investigate can present all processed and filtered data from Nuix workstation. The platform will allow NFCU users to concurrently and collaboratively review the data in a user-friendly and analytical environment. Comments and decisions made by one reviewer can be seen by another for transparent review and to prevent review duplication. Data is categorised into file types for ease of identification and our experienced analysts provide user training for NFCU reviewers to ensure they get the most out of the platform's capabilities. NFCU reviewers could access the review platform from their own work issued desktop or laptop computers. CCL manage secure access through user credentials, two factor authentication and IP address allow lists enabling reviewers to access the platform from work or home.
10) CCL's remote viewing service is built upon Microsoft Azure infrastructure and the Nuix Investigate software. This is a well-established service that CCL have been successfully providing to Law Enforcement clients since 2019.
11) Nuix Investigate presents data from a multitude of sources, enabling concurrent and collaborate review of data in a user-friendly, analytical environment. The intuitive interface allows users to search through the dataset using a variety of means such as date ranges, complex keywords, file types and metadata (file information).
12) An advanced query builder function provides the means for reviewers to construct detailed searches and save for later use. CCL's analyst support team are highly skilled in the customizing of search criteria and can assist reviewers in building saved searches for future use. The platform can also be scaled to allow any number of reviewers to simultaneously access a case. Comments and decisions made by one reviewer can be seen by another for transparent review and to prevent review duplication. Data can be completely segregated for data subject to legal privilege. CCL will provide access to users assigned to specific case with specific access rights.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

13) There is Two Factor Authentication on Azure service user profiles, that sends a text message to the user's phone once they successfully enter their credentials. This securely provides access to the web front-end logon screen and permitted case files.
14) Data is protected between the end-user's web browser and Nuix by an issued SSL Certificate, which encrypts the data transfer. The infrastructure for Nuix is in its own segregated virtual network and subnet from any other cloud services, allowing only the Nuix infrastructure to communicate with its own resources. Data is stored and backed up within the Azure Infrastructure across Virtual Machines and Storage Accounts. CCL only use accredited UK-based data centres. Azure holds a wide range of accreditations.
15) CCL will provide NFCU with the number of licenses requested per case, these can be used simultaneously. A booking system could allow NFCU to allocate licenses to specific cases for a set duration. CCL will provide dedicated licensing to NFCU and dependent data volumes and the number of reviewers required, the license pool can be scaled.
16) CCL's analysts will be able to access the casefiles at the same time as NFCU and therefore provide real time support over the phone or through screen share. Our analysts will also be able to attend NFCU offices to offer further support or training should it be required. The review service is typically available on a 24/7 basis, although CCL would inform NFCU as soon as possible if any un-planned maintenance to the review system were required and endeavour to perform this outside of standard UK business hours. Our support team would be available via telephone within standard UK business hours. Out of hours support is available as an additional billable service.

Production

1) Following the successful conclusion of a review and identification of relevant evidence and unused material the lead DA Team examiner ascertains production requirements with the lead NFCU investigator. Those requirements could include the production of evidence in a technical 'Load File' format for disclosure to other parties eDisclosure provider(s) or in an accessible 'eBundle' format. CCL has assisted many Law Enforcement clients with an 'eBundle' production, consisting of a spreadsheet containing basic file and communication metadata (e.g. file name, file path and email; sender, subject and sent time) in the header columns with a row to describe each item. Hyperlinks in the spreadsheet for each row link to an item; native copy, extracted text, PDF conversion and a report detailing all metadata. Additionally, each row item is ascribed a document reference (e.g. 'ID-PROD1-000001') with any child items allocated subsequent references. The PDF conversion of an item can be stamped with document references and their page numbers. A range of other options for endorsing PDF conversions are available. The metadata can also include names and paths of duplicate evidential files from the whole Nuix case rather than just the review subset.
2) The items in the Production could be easily be made available to a reviewing lawyer alongside a case summary for remote case consideration without the need to physically print evidential material.
3) Should a subset production be required for Court presentation CCL can easily create this by reference to a list of Document Reference identifiers (and/or their page numbers) in the original production and apply custom endorsements and pagination as required to present a Court or Jury Bundle for distribution and remote review or printing.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

4) CCL can deliver hard copy productions on digital media or by a secure electronic file share service.
5) Witness statements can be provided to describe each stage of an examination, including mobile extraction, imaging, analysis and processing. As a standard procedure CCL disclose evidential chain of custody continuity information and examination notes in a case disclosure schedule. For the Scenario CCL would expect to provide statements covering; scene examination, mobile extraction and computer/storage imaging, plus an overarching case conduct statement describing all CCL activities including a summary of imaging and extraction activities, data processing in Nuix, analysis (including LPP and other searches), review provision and conduct and production of evidential data as an exhibited eBundle or Load File. CCL evidence is subject to rigorous internal scrutiny and quality assurance before release to a client.

Presentation

1) Data described and produced by CCL as an exhibit in a Load File or eBundle is provided with an evidence reference as per the exhibiting statement. Each item with an exhibit (e.g. individual text messages, an email or an email attachment) is as previously described allocated a unique reference. Exhibit references could be tailored to suit NFCU preferences. CCL standard practice is to sequentially associate exhibit references with the examiner, case reference and date. By way of example the first production of items in case 'NFC1008105' with references 'ID-PROD1-0000001' to 'ID-PROD1-000572' made by an examiner with initials 'ANE' on 20 July 2020 would be 'NFC1008105/ANE/001/001-572/20200720'.
2) Page nine of the PDF converted copy of the first document in the first production could be endorsed with 'ID-PROD1-000001' in the top left corner and '009' in the top right corner. Subsequent productions could be exhibited with increments in the production reference, '002', '003' etc and follow on increments in the production ID references, e.g. '573-894' and relevant suffixed dates. The second production made by the same examiner on 28 July 2020 would be 'NFC1008105/ANE/002/573-894/20200728' in this notation scheme.
3) CCL could if required identify the Production ID reference items in the case, following internal or external legal review of productions either by applied Nuix tags from remote review or a list of references from hard copy review. Once all items were identified a PDF bundle of relevant material could be assembled by CCL, endorsed at the top of each page with a production ID reference, exhibit reference and page number and in the bottom right of each page with a running presentation pagination number. If required CCL could hard print Jury Bundles or make items available electronically via the PDF copy only displayed in Nuix Investigate or another review platform.
4) With overnight warning (subject to advanced notice of trial period) CCL witnesses can attend any Court in the UK. Extraction, imaging and the overarching statements provided by the lead CCL examiner for the case would be provided on a factual basis professional witness basis. CCL also has many senior examiners who can provide evidence of opinion, based on established facts ascertained in a detailed examination. CCL experts regularly provide evidence in relation to Digital Forensics, Incident Response (hacking and intrusion) and Cell Site analysis.

Data Storage and Decommissioning

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

1) While the case is active there are no charges for storage of images, extractions, other collected data or Nuix case data beyond review hosting charges.
2) Following the production of evidence CCL can continue hosting the review for NFCU to access or transfer it to online archive storage.
3) Hosting provides instant access and archive storage takes 48hrs to restore to review.
4) On case completion CCL can decommission the case and return to NFCU for storage on hard media, via shared file or cloud transfer.
5) CCL provide an alternative solution allowing for longer term storage of the case data, collected imagers and extractions in CCL's Azure hosted 'cold' storage facility. Restoration to review is still possible and enables clients to meet their own retention policies and ongoing disclosure obligations following a successful prosecution. Azure Cloud offline deep storage is very cost effective and CCL are confident that it provides a better value for money option than equivalent on premise backed up data or server storage options.

B. Deliverables

Please outline the proposed scenario milestones and deliverables. Please provide a timetable of key dates or significant events for the scenario (for example fieldwork dates, dates for provision of research materials, draft and final reporting). Deliverables must be linked to any objectives.

For larger or more complex projects please insert as many deliverables /milestones as required.

Each deliverable should be:

i. no more 100 characters in length
ii. self-explanatory
iii. cross referenced with objective numbers i.e. deliverables for Objective 1 01/01, 01/02 Objective 2 02/01, 02/02 etc

Please insert additional rows to the table below as required.

Deliverable	Target	TITLE of Deliverableor milestone
1.	Week 1/2	Scene attendance, return of the Exhibits to CCL, all imaging and extractions work completed.
2.	Week 2/3	DA team Processing of the Exhibits.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

3.	Week 3	Specialist processing of Log Label Data and online provision to NFCU/Machine manufacturer(s)
4.	Week 3	Searching and identification of the Case Data to identify the Review Data
5.	Week 4	Reporting of final search results and online access review provision for NFCU Investigators to the Review Data.
6.	Weeks 4-8	(dependant on data volumes) completion of the Review by NFCU.
7.	Week 5 onwards	CCL collation and provision of the Production draft for NFCU approval
8.	Week 6 onwards	CCL supply of production evidence and statements
9.		

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

THE SCENARIO - EXPERTISE and STAFF EFFORT	
D. Named Staff Members THAT will be needed for the scenario and Details of their Specialism and expertise	
Please give the names and grades of all staff who will work on the scenario together with details of their specialism and expertise, their role in the project. If new staff will be hired to deliver the project, please detail their grade, area/(s) of specialism and their role in the project team.	
Lead Applicant	CCL-Forensics
Named staff members, details of specialism and expertise.	
Please see provided profiles	
Participant Organisation 1	
Named staff members, details of specialism and expertise.	
Participant Organisation 2	
Named staff members, details of specialism and expertise.	
Participant Organisation 3	
Named staff members, details of specialism and expertise.	

E. STAFF EFFORT

In the table below, please detail the staff time to be spent on the scenario (for every person named in section above) and their role in delivering the proposal. If new staff will be hired in order to deliver the project please include their grade, name and the staff effort required.

Name and Role of Person where known/ Role of person to be recruited	Working hours per staff member on this project
Principal Analyst (Data Analytics)	10
Analyst (PC)	48
Analyst (Mobile)	30
Analyst (Data Analytics)	49

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Technician (Data Analytics & PC)	17
Senior Analyst (On Site)	42
Senior Analyst (Data Analytics)	50
Total staff effort	246

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

THE SCENARIO - PROJECT MANAGEMENT

Please fully describe how the project will be managed to ensure that objectives and deliverables will be achieved on time and on budget. Please describe how different organisations/staff will interact to deliver the desired outcomes.

Highlight any in-house or external accreditation for the project management system and how this relates to this project.

Project Commencement

On engagement CCL/NFCU would schedule an exploratory scoping call to check the requirements of the provided NFCU Work Package. The deliverable from this is a Forensic Strategy and Programme of Work (please see documents 4.A. Forensic Strategy and Programme of Work). These form the Project Initiation documentation.

Project Governance

Each client is assigned a dedicated CCL Forensic Case Team (“FCT”) contact who manages all aspects of exhibit submission, retention and return. A named member of each laboratory team co-ordinates their respective activities and dependent on the case type an overall internal CCL lead for a multidisciplinary case is appointed. This person is responsible for maintaining contact with the lead client case investigator and will update to confirm tasks such as completion of imaging, triage, processing, review readiness and evidence production. The list is not exhaustive and regular communication between the client and CCL lead is expected on regular basis as the case progresses. CCL provide email, landline and mobile contact details at the commencement of an engagement to assure effective and accessible client communication. In the Scenario the CCL case team lead would be a Consultant or Project Manager on the DA Team.

Cases are also managed corporately by maintaining electronic records within a case management system. Regular Operations Meeting allow for the recognition and mitigation of any potential resourcing issues (technology or people).

Change Control

It is possible that as a case progresses, new factors will emerge. These can include the requirement for advanced analysis, more analysis time than originally estimated being required or findings that seem significant given the case strategy. As soon as the scope of the enquiry changes or the lead analyst becomes aware that the case will require more time than originally estimated, they will discuss this with the client. With new lines of enquiry, this will involve weighing time constraints against the value of any additional evidence sought. Where the issue is the volume of the evidence found, the analyst will agree a strategy that achieves the evidential objectives in the timeliest and most cost-effective way. Where significant findings have been made, we would discuss the best way of providing those findings in a timely manner.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

No additional work is undertaken without appropriate customer approval.

THE SCENARIO - RISK MANAGEMENT

In the table provided, please identify all relevant risks in delivering this project on time and to budget. Briefly outline what steps will

Please add more lines as required

CCL have provided risks related to Project Management, technical limitations and assumptions are documented as part of our met

Identified risk	**Likelihood o**
Client requirements not fully understood. Resulting in deliverables not being as required	Low
Cost of delivering required scope exceeds budget allocated	Low
Lack of appropriate people from NFCU available in timely fashion who are empowered to make decisions on behalf of the investigation	Low
Failure of CCL hardware/software/infrastructure	Low
Failure to provide sufficient people resource	Low

CCL has completed a Risk Register related to working during COVID-19, which is available if required

INVESTIGATIVE REVIEW PLATFORM

In the below space please give accurate details of what Investigative review platform will be provided with the p and how this meets the needs of the NFCU. This should include, but not limited to;

- Licencing needs or requirements
- Support either online, in person, via telephone
- How multiple Investigators can work on the case from multiple locations

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

CCL's remote viewing service is built upon Microsoft Azure infrastructure and the Nuix Investigate software. This is a well-established service that CCL have been successfully providing to Law Enforcement clients over the past year.

Investigate presents data from a multitude of sources. The platform allows for remote, concurrent, collaborate review of data in a user-friendly, analytical environment. The intuitive interface allows users to search through the dataset using a variety of means such as date ranges, complex keywords, file types and metadata (file information). An advanced query builder function provides the means for reviewers to construct detailed searches and save for later use. CCL's analyst support team are also highly skilled in the customizing of search criteria and can assist reviewers in building saved searches for future use. The platform can also be scaled to allow any number of reviewers to simultaneously access a case. Comments and decisions made by one reviewer can be seen by another for transparent review and to prevent review duplication. Data can be completely segregated for data subject to legal privilege. CCL will provide access to users assigned to specific case with specific access rights.

There is Two Factor Authentication on Azure service user profiles, that sends a text message to the user's phone once they successfully enter their credentials. This securely provides access to the web front-end logon screen and permitted case files.

Data is protected between the end-user's web browser and Nuix by an issued SSL Certificate, which encrypts the data transfer. Customers are whitelisted using the IP address they utilise to access the service. Reviewers will use their own computers to access the service from any location by providing their IP address. The infrastructure for Nuix is in its own segregated virtual network and subnet from any other cloud services, allowing only the Nuix infrastructure to communicate with its own resources. Data is stored and backed up within the Azure Infrastructure across Virtual Machines and Storage Accounts. CCL only use accredited UK-based data centres. Azure holds a wide range of accreditations.

CCL will provide NFCU with the number of licenses requested per case, these can be used simultaneously. A booking system will allow NFCU to allocate licenses to specific cases for a set duration. CCL will provide dedicated licensing to NFCU and dependent data volumes and the number of reviewers required, the license pool can be scaled.

CCL's analysts will be able to access the casefiles at the same time as NFCU and therefore provide real time support over the phone or through screen share. Our analysts will also be able to attend NFCU offices to offer further support or training should it be required. The service is typically available on a 24/7 basis. CCL will inform NFCU as soon as possible if any un-planned maintenance to the review system is required and we endeavour to perform this outside of standard UK business hours. Our support team will be available via telephone within standard UK business hours. Out of hours support is available as an additional billable service.

Following the review of data, CCL are able to customise the output to meet NFCU requirements. Should data be required to send to another party to ingest into a review platform, CCL can liaise directly to agree on a format. Alternatively, should a production of relevant data be required that can be accessed outside of a review platform, CCL can provide the files with unique references alongside a spreadsheet containing all the file information and a clickable link to the actual file or PDF representation. The final productions can be provided on hard copy media or shared electronically via CCL's secure file transfer site. Witness statements can be provided to produce the exhibits and identify all continuity procedures. During the review, it can be possible to provide NFCU with the ability to download files as they review or to export PDF representations of the files.

Following the review of data, CCL can keep hosting the case file for NFCU to access, this will attract an ongoing monthly hosting fee. Alternatively, CCL can move the case file to our archive storage which will allow the case file to be made accessible within two days of access request, this will attract an ongoing archive fee. Should the case be complete, CCL can decommission the

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

case and return to NFCU for storage. Should any further work be required on the case, NFCU can return the data to CCL for reinstating onto the review platform. All actions carried out within the Nuix software are recorded. As a result, it is possible to provide an audit trial for the processing, analysis, review and export of the data. Alongside this, CCL keep contemporaneous notes in line with ISO17025 standards that outlines the steps taken to provide the data for review.

DESCRIPTION OF THE ISO17025 ACREDITED PROCESSES

In the table below please list which processes are approved and accredited by UKAS ISO

Materials/Products tested	**Type of test/Properties measured/Range of measurement**	**Standard specifications/ Equipment/Techniques used**	**Further info if required**
	Forensic Testing	The organisation has demonstrated adherence to the relevant requirements of the Forensic Science Regulators Code of Practice and Conduct in relation to their Forensic Activities	
COMPUTERS AND DIGITAL STORAGE DEVICES *(Internal and External Computer Hard Disks, Memory Cards, USB Sticks, Compact Discs, Digital Versatile Discs, Floppy disks, MP3/4 players, Digital Cameras)*	*Capture and Preservation of Digital Data (Forensic Copy)*	Documented in-house methods (SOP 6, SOP 147 and SOP148) using the following 3rd party hardware and software examination tools : - Encase - FTK Imager - MacQuisiton - Paladin - Raptor - A range of Hardware Forensic Write Blockers	*Example - In house SOP 1, 2, 3, 4*
Data associated to the following operating systems : - MS Windows - Apple - Linux	Extraction and analysis of data from digital media	Documented in-house methods (SOP 8, SOP86, SOP145, SOP196, SOP197 and SOP201) using the following 3rd party hardware and software examination tools : - Encase (Linux excluded) - FTK (Linux excluded) - Internet Evidence Finder (Linux excluded) - C4ALL (Linux excluded) - Nuix - Blacklight - Axiom - Griffeye	Of particular note to this requirement, CCL is currently the only provider with Nuix in scope

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

		- X-Ways (incuding Jedson-extension) - Ribbon	
Mobile Phone Handsets, Tablets (U)Sim Cards and associated memory cards	Logical capture and preservation of data (SIM Card, Handset, Tablets)	Documented in-house methods (SOP41) using manual extraction and the following 3rd party data extraction software: - XRY - Cellebrite UFED Touch - UFED Physical Analyzer (SIM not included) - Aceso (SIM only) - Encase - C4All - Ribbon - Dunk! - X-Ways - Internally developed scripts: - iOS_SMS_iMessage.py - iOS_WhatsApp.py - Android_Messages.py - Android_WhatsApp.py	
Mobile Phone Handsets, Tablets (U)Sim Cards and associated memory cards	Physical capture and preservation of data (Handset, Tablets, Memory Card)	Documented in-house methods (SOP41) using the following 3rd party data extraction software: - XRY (including XACT) - Cellebrite UFED Touch - UFED Physical Analyzer – (memory card excluded) - FTK Imager (Memory cards only) - Encase - C4All - Ribbon - Dunk! - X-Ways - Internally developed scripts: - iOS_SMS_iMessage.py - iOS_WhatsApp.py - Android_Messages.py - Android_WhatsApp.py	
SATELLITE NAVIGATION SYSTEMS (TomToms and Garmin)	Capture and preservation of data from ‘Sat-Nav’ devices	Documented in-house methods (SOP11, SOP 41, SOP173, SOP179 and SOP176) using manual extraction and the following In-house developed or 3rd party software tools: - FTK Imager - Tomtology 1 and Tomtology 2	

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

ADDITIONAL SUPPORTING DOCUMENTS

Please note that any additional documents in support of the on-line application, as well as the Gant/PERT charts requested for the Project Plan section, should be zipped into a single file (using WinZip). These should then be uploaded to the e-sourcing portal, Bravo in to the *Supporting Documents* section of the technical envelope. Each supporting document should be clearly marked with the following details:

- the tender reference number,
- the tender title,
- the name of the lead applicant submitting the proposal and
- the part number and title to which the supporting evidence appertains (e.g. Part 3 Deliverables)

Index of Supporting Documents

Q number	Document
1.B.	FS900084_Digital Forensics_CCL-F_1B_Staff Profiles (Examples)
3.A	FS900084_Digital Forensics_CCL-F_3A_Schedule of Accreditation
3.B	FS900084_Digital Forensics_CCL-F_3B_Environmental policy
3.B	FS900084_Digital Forensics_CCL-F_3B_Equal Opportunities policy
3.D	FS900084_Digital Forensics_CCL-F_3D_Information Security Management Policy
3.D	FS900084_Digital Forensics_CCL-F_3D_Security Incident Reporting Policy
4.A	FS900084_Digital Forensics_CCL-F_4A_Forensic Strategy
4.A	FS900084_Digital Forensics_CCL-F_4A_Programme of Work
4.A	FS900084_Digital Forensics_CCL-F_4A_Gannt Chart
4.D	FS900084_Digital Forensics_CCL-F_4D_Staff Profiles (Scenario)

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

Clarification Questions and Answers

Q1. Please confirm the daily and hourly rate for each of the roles included in the staff costs table and rate card. The Staff Costs table appears to include hourly rates rather than daily rates and the maximum daily rate in the Rate Card does not contain the maximum daily rate.

A1. Apologies for the oversight regarding the hourly/day rate.

Please Note:
Because the minimum unit for a day rate is 0.25, offering the pricing as a day rate rather than an hourly rate has resulted in a small increase in the bid price

It was stated in the feedback that "a narrative was provided for potential T & S costs – these were not included in the bid." These were actually listed in the Consumables and Other Costs Tab and are:

NUIX Usage Charge
Azure Data Hosting
Review User Licenses

Costs provided assume 2 x reviewers for one month.

Updated Financial Templated included in this Framework Agreement.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Schedule 6 (Work Package Call Off Procedure and Order Form)

Work Package Call Off Procedure

Work Packages can only be called off Framework FS900084 Digital Forensic if the work relates to the overarching Framework Contract and the specification that was used to tender for this.

Any Work packages cannot begin until the work package call off has been signed by both the supplier and Procurement. This is to protect both the FSA and the Supplier. Suppliers are working at risk until they have a signed WP with no guarantee of payment, whilst the FSA carries unmanaged risk around confidentiality, insurance, GDPR and is potentially breaking the law if agreeing to proceed work without a contract.

The NFCU Lead must approach the Knowledge Information Management Team regarding the work before the Request for Quotation (RFQ) to discuss any GDPR implications and whether there is a requirement to complete a Personal Impact Assessment (PIA) / mini PIA to feed into the RFQ.

Work Package Procedure:

1 - Formal request for Quotation form sent to Supplier.

This should include specification of requirements, what the outputs will be used for and any GDPR personal data & data subjects that may/will be processed by the supplier as part of the requirement.

2 – Supplier responds to requestor within 48 hours with proposal.

This can be on FSA standard Work Package template annex 1 or in the Suppliers own template but must clearly indicate it is subject to the terms and conditions of the overarching Framework Contract and contain:

- Call Off contract reference and name
- A detailed methodology of how they will deliver the requirement.
- Clear timescales – Final delivery date, any milestones etc.
- Any equipment, network access, staff access that the supplier requires from the FSA to carry out the work.
- Any assumptions the supplier has made in their response.
- Any risks identified and how these will be managed.
- Clear detailed costings of the proposal, including a breakdown of the roles, day rates (no greater than the rate card prices for the framework)and number of days roles will work, any expected expenses (in line with the framework) and any other costs, such as licenses. It should also include the charging method (fixed, capped time and material etc.) and where applicable milestone payments should be attributed to deliverables.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

- GDPR schedule indicating how any personal data will be processed, nature of why it is being processed, how long it will be processed for, plan for return/destruction of data etc.
- Overall Call-Off value.

The work package should include all the information required and not refer to linked documents, attachments, slides etc.

3 – NFCU lead will review the Work Package to ensure it contains all the required information and confirm that funds are in place for this work.

4 – Once funding is confirmed and Procurement and business are happy with the WP then it will be accepted, and the NFCU lead will arrange for both supplier and Procurement to sign it off. A PO can then be raised. Either by NFCU or by CSU.

Annex 1

FS900084

Request for Quotation

FS900084 – Digital Forensic Provider Framework
Work Package Number:
Work Package Title:
Supplier Name:
Specification of requirements – (to be completed by FSA)
Supplier response – please provide a detailed methodology of how you will deliver the requirements
Delivery timescales – Please provide a detailed plan of when you will deliver the specified outcomes
Please detail any assumptions you have made
Please detail any identified risks and your proposed mitigation measures
Costings – Please provide a detailed breakdown of all costs to deliver the specified requirements
GDPR - Processing, Personal Data and Data Subjects

Description	Details
Identity of Controller for	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with the overarching Framework Contract, (Where the Party is a

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

each Category of Personal Data	Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: • ***[Insert** the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Buyer*
Duration of the Processing	*[Clearly set out the duration of the Processing including dates]*
Nature and purposes of the Processing	*CCL will be a data processor for the purposes of this contract. We will be extracting data from digital devices (potentially including personal devices) and we will be storing personal data from these Devices.* *Transmission will be to FSA authorised personnel only* *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, erasure or destruction of data (whether or not by automated means) etc.*

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	The purpose might include: employment processing, statutory obligation, recruitment assessment etc]
Type of Personal Data	*Data could include anything that might be found on a digital device including name, address, DOB, contact details, correspondence, application data, images and video*
Categories of Data Subject	*Suspects under investigation and owners/custodians of devices seized during an investigation*
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	*Extracted data will be retained for 6 months following completion of the forensic services.* Following which it will be securely destroyed or provided to FSA in its entirety for their storage. Case related data (contemporaneous notes, continuity documentation and communication records) will be stored for 7 years.

Completed by:
Date:
Call Off - Call off work package acceptance
Date quotation accepted by FSA:

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Work Package start date:
This quotation for the above mentioned Work Package has been agreed between the Food Standards Agency and the Supplier under the terms and conditions of the Framework Contract FS900084 – Digital Forensic Provider Framework Signed on behalf of the FSA Procurement Name: Signature:_____ Position: Date: Signed on behalf of the Supplier Name: Signature:_____ Position: Date:

Schedule 13 (Framework and Work Package Call Off Contract Management)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Schedule 1 (Definitions):

"Operational Board"	the board established in accordance with paragraph 4.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

2. Project Management

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Framework Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day throughout the Framework Contract Period.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Framework Contract and Work Package Call Off can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. Role of the Supplier Project Manager

3.1 The Supplier Project Manager shall be:

3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;

3.1.2 the supplier shall put in place a structure to manage this Contract in accordance with Framework Schedule 2 (Specification) and the Performance Indicators.

3.1.3 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Project Manager's responsibilities and obligations;

3.1.4 able to cancel any delegation and recommence the position himself; and

3.1.5 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Project Manager in regards to the Framework Contract and it will be the Supplier Project Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier Project Manager by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. Role of The Operational Board

4.1 The Operational Board shall be established by the Buyer for the purposes of this Framework Contract on which the Supplier and the Buyer shall be represented.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in Annex A to the Schedule.

4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Framework Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5. Contract Risk Management

5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Framework Contract.

5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

5.2.1 the identification and management of risks;

5.2.2 the identification and management of issues; and

5.2.3 monitoring and controlling project plans.

5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

5.4 The Supplier will maintain a risk register of the risks relating to the Framework Contract which the Buyer and the Supplier have identified.

6. How the Supplier's Performance will be measured

At the end of each project the buyers project lead will complete a report detailing:

- Any delays within the project, how long the delays were and if they were communicated with the buyer.
- What the delays and if they were outside the suppliers control.
- Was the project delivered fully and how satisfied was the buyer with the overall project on scale of 1-5. 5 been extremely satisfied and 1 been not at all satisfied.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Annex: Operational Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

If there are any significant issues flagged in any project, then a board meeting will be called the locations to be agreed at the time.

Schedule 16 (Security)

Security Management Schedule

In this Schedule:

Authority	is Food Standards Agency
Authority Data	(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: a. supplied to the Supplier by or on behalf of the Authority; and/or b. which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or (b) any Personal Data for which the Authority is the Data Controller;
Breach of Security	an event that results, or could result, in: (c) any unauthorised access to or use of the Authority Data, the Services and/or the Information Management System; and/or (d) the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including any copies of

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	such information or data, used by the Authority and/or the Supplier in connection with this Agreement;
CHECK Service Provider	means a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the ITHC services required by the Paragraph **Error! Reference source not found.** of this Schedule
Certification Requirements	means the information security requirements set out in paragraph 5 of the Security Management Schedule
Incident Management Process	is the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Authority Data, the Authority, the Services and/or users of the Services and which shall be shall be prepared by the Supplier in accordance with Paragraph 4 of this Schedule (Security Management)

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Information Management System	comprises: (i) the Supplier Equipment; (ii) the Supplier System; and (iii) the Sites at which Authority Data is held
ITHC	has the meaning given in Paragraph 7.1.1 of this Schedule (Security Management);
Personal Data	has the meaning given in the Data Protection Legislation;
Personal Data Breach	has the meaning given in the Data Protection Legislation;
Personal Data Processing Statement	sets out: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Subcontractors Process Authority Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Authority Data against a Security Breach including a Personal Data Breach, which shall be prepared by the Supplier in accordance with Paragraph 4 of this Schedule (Security Management)
Process Authority Data	any operation which is performed on Authority Data, whether or not by automated means, including adapting, altering, collecting, combining, copying, destroying, erasing, organising, publishing retrieving, storing,

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	structuring, transmitting or otherwise using Authority Data;
Protective Measures	appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it
Sites	comprise: (i) those premises from which the Services are to be provided; (ii) those premises from which Supplier manages, organises or otherwise administers the provision of the Services; and, (iii) those premises at which any Supplier Equipment or any party of the Supplier System is located.
Supplier Equipment	the hardware, computer and telecoms devices and equipment used by the Supplier or its Subcontractors (but not hired, leased or loaned from the Authority) for the provision of the Services;
Supplier System	the information and communications technology system used by the Supplier in implementing and performing the Services, including the Software, the Supplier Equipment, configuration and management utilities, calibration and testing

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Crown Copyright 2019

	tools and related cabling (but excluding the Authority System);
Vulnerability Management Policy	A policy that defines the Supplier's approach and process for identifying vulnerabilities conducting risk assessments and patching.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

2. Introduction

2.1 This Schedule addresses:

2.1.1 the arrangements which the Supplier shall implement and comply with when performing its obligations under this Agreement and/or providing the Services in order to ensure the security of the Authority Data;

2.1.2 the Certification Requirements applicable to the Supplier and each of those Sub-contractors which Processes Authority Data;

2.1.3 The security requirements in Annex 1 to this Schedule which the Supplier must comply with;

2.1.4 the tests which the Supplier shall conduct on the Information Management System during the Term in Paragraph 7;

2.1.5 the Supplier's obligations to:

(a) return or destroy Authority Data on the expiry or earlier termination of this Agreement; and

(b) prevent the introduction of Malicious Software into the Service and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Services in Paragraph 9; and

(c) report Breaches of Security to the Authority.

3. Principles of Security

3.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of the Information Management System.

3.2 Notwithstanding the involvement of the Authority in assessing the arrangements which the Supplier shall implement in order to ensure the security of the Authority Data, the Supplier shall be, and shall remain, responsible for:

3.2.1 the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors;

3.2.2 the security of the service and Supplier System provided to host Authority evidential data.

3.3 If required the Supplier shall provide the Authority with access to members of its information assurance personnel to facilitate the Authority's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

4. Information Security Governance Policies

4.1 The Supplier shall prepare and submit to the Authority within 20 Working Days of the date of this Agreement:

4.1.1 A statement that it has conducted a CHECK IT Health Check of the Supplier System during the last year;

4.1.2 the Personal Data Processing Statement;

4.1.3 A copy of the Supplier Incident Management Process; and

4.1.4 A copy of the Vulnerability Management policy.

5. Compliance Reviews

5.1 The Supplier shall notify the Authority within 5 Working Days after becoming aware of:

5.1.1 a significant change to the components or architecture of the Service;

5.1.2 a new risk to the components or architecture of the Service;

5.1.3 a vulnerability to the components or architecture of the Service which is classified 'Medium', 'High', 'Critical' or 'Important' in accordance with the classification methodology set out in section 19 of Annex 1 to this Schedule;

5.1.4 a change in the threat profile;

5.1.5 a significant change to any risk component;

5.1.6 a significant change in the quantity of Personal Data held within the Service;

5.1.7 a proposal to change any of the Sites from which any part of the Services are provided; and/or

5.1.8 an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

5.2 Where the Supplier is required to implement a change in order to remedy any non-compliance with this Agreement, the Supplier shall effect such change at its own cost and expense.

6. Certification Requirements

6.1 The Supplier shall be, and shall ensure that each Sub-contractor which Processes Authority Data is compliant with:

6.1.1 ISO/IEC 27001:2013 by a UKAS approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

6.1.2 Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or Process Authority's Data. Any exceptions to the flow-down of the certification requirements to third party suppliers and sub-contractors must be agreed with the Authority.

6.2 The Supplier shall ensure, at all times during the Term, that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:

6.2.1 securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

6.2.2 are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority.

6.3 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph before the Supplier or the relevant Sub-contractor (as applicable) may carry out the secure destruction of any Authority Data.

6.4 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-contractor shall:

6.4.1 immediately ceases using the Authority Data; and

6.4.2 procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with the requirements set out in this Paragraph.

7. Security Testing

7.1.1 The Supplier shall ensure at its own cost and expense procure and conduct an IT Health CHECK ("**ITHC**") of the Supplier System by a CHECK Service Provider at least on an annual basis

7.1.2 If requested provide the Authority with a copy of the IT Health Check report;

8. Security Monitoring and Reporting

8.1 The Supplier shall:

8.1.1 monitor the delivery of assurance activities;

8.1.2 monitor security risk impacting upon the operation of the Service;

8.1.3 report Breaches of Security in accordance with the approved Incident Management Process (see 4.1.3).

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

9. Malicious Software

9.1 The Supplier shall install and maintain anti-Malicious Software or procure that anti-Malicious Software is installed and maintained on any part of the Service which may Process Authority Data and ensure that such anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

9.2 If Malicious Software is found, the parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

9.3 Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 9.2 shall be borne by the parties as follows:

9.3.1 by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier or the Authority Data (whilst the Authority Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Authority when provided to the Supplier; and

9.3.2 by the Authority, in any other circumstance.

10. Breach of Security

10.1 If either party becomes aware of a Breach of Security it shall notify the other in accordance with the Incident Management Process (see 4.1.3).

10.2 The Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:

10.2.1 Immediately take all reasonable steps necessary to:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible;

(c) apply a tested mitigation against any such Breach of Security; and

(d) prevent a further Breach of Security in the future which exploits the same root cause failure;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

10.2.2 as soon as reasonably practicable and, in any event, within 2 Working Days, following the Breach of Security or attempted Breach of Security, provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

10.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Subcontractors then such remedial action shall be completed at no additional cost to the Authority.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Annex 1: Security Requirements

11. Security Classification of Information

The provision of the Service requires the Supplier to Process Authority Data which is classified as OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

12. End User Devices

12.1 The Supplier shall ensure that any Authority Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority except where the Authority has given its prior written consent to an alternative arrangement.

12.2 The Supplier shall ensure that any device which is used to Process Authority Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

13. Networking

The Supplier shall ensure that any Authority Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

14. Personnel Security

14.1 All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.

14.2 The Authority and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Authority Data or data which is classified as OFFICIAL-SENSITIVE.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

14.3 The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 14.1 and 14.2 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

14.4 The Supplier shall ensure that Supplier Personnel are only granted such access to Authority Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.

14.5 The Supplier shall ensure that Supplier Personnel who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within 1 Working Day.

15. Identity, Authentication and Access Control

15.1 The Supplier shall operate an access control regime to ensure:

15.1.1 all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and

15.1.2 all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

15.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.

15.3 The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Authority on request.

16. Data Destruction and Deletion

The Supplier shall:

16.1 prior to securely sanitising any Authority data or when requested the Supplier shall provide the Authority with all Authority Data in an agreed open format;

16.2 have documented processes to ensure the availability of Authority Data in the event of the Supplier ceasing to trade;

16.3 securely erase in a manner agreed with the Authority any or all Authority Data held by the Supplier when requested to do so by the Authority;

16.4 securely destroy in a manner agreed with the Authority all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Agreement and, in the absence of any such requirements, in accordance with Good Industry Practice as agreed by the Authority; and

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

16.5 implement processes which address the CPNI and NCSC guidance on secure sanitisation.

17. Audit and Protective Monitoring

17.1 The Supplier shall collect audit records which relate to security events that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Supplier System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.

18. Location of Authority Data

The Supplier shall not and shall procure that none of its Sub-contractors Process Authority Data outside the EEA without the prior written consent of the Authority and the Supplier shall not change where it or any of its Sub-contractors Process Authority Data without the Authority's prior written consent may be subject to conditions.

19. Vulnerabilities and Corrective Action

19.1 The Authority and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Authority Data.

19.2 The severity of vulnerabilities for Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier as ‘Critical’, ‘Important’ and ‘Other’ by aligning these categories to the vulnerability scoring according and using the appropriate vulnerability scoring systems including:

19.2.1 the ‘National Vulnerability Database’ ‘Vulnerability Severity Ratings’: ‘High’, ‘Medium’ and ‘Low’ respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and

19.2.2 Microsoft’s ‘Security Bulletin Severity Rating System’ ratings ‘Critical’, ‘Important’, and the two remaining levels (‘Moderate’ and ‘Low’) respectively.

19.3 Subject to Paragraph 19.4, the Supplier shall procure the application of security patches to vulnerabilities in the Core Information Management System within:

19.3.1 7 days after the public release of patches for those vulnerabilities categorised as ‘Critical’;

19.3.2 30 days after the public release of patches for those vulnerabilities categorised as ‘Important’; and

19.3.3 60 days after the public release of patches for those vulnerabilities categorised as ‘Other’.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

19.4 The timescales for applying patches to vulnerabilities in the Core Information Management System set out in Paragraph 19.3 shall be extended where:

19.4.1 the Supplier can demonstrate that a vulnerability in the Core Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 19.3 if the vulnerability becomes exploitable within the context of the Services;

19.4.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

19.5 the Authority agrees a different maximum period after a case-by-case consultation with the Supplier

19.6 The Supplier will provide a copy of the Vulnerability Management policy covering the provisions for major version upgrades of all Supplier COTS Software and Third Party COTS Software to be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing.

20. Secure Architecture

20.1 The Supplier shall design the Information Management System in accordance with:

20.1.1 the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main;

20.1.2 the NCSC "Bulk Data Principles", a copy of which can be found at https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and

20.1.3 the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:

(a) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

(b) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

(c) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

(d) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;

(e) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;

(f) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;

(g) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;

(h) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;

(i) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;

(j) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;

(k) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;

(l) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;

(m) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors; and

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

(n) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Schedule 20 (Processing Data)

Status of the Controller

1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA. A Party may act as:

(a) "Controller" in respect of the other Party who is "Processor";

(b) "Processor" in respect of the other Party who is "Controller";

(c) "Joint Controller" with the other Party;

(d) "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

2. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

3. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

4. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

5. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Framework Contract:

(a) Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not Process Personal Data except in accordance with the Framework Contract (and in particular Annex 1 *(Processing Personal Data*));

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this Schedule 20, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);

(B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Framework Contract; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Framework Contract unless the Processor is required by Law to retain the Personal Data.

6. Subject to paragraph 7 of this Schedule 20, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Framework Contract it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Framework Contract;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Personal Data Breach.

7. The Processor's obligation to notify under paragraph 6 of this Schedule 20 shall include the provision of further information to the Controller, as details become available.

8. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Schedule 20 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

(d) assistance as requested by the Controller following any Personal Data Breach; and/or

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

9. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Schedule 20. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the Processing is not occasional;

(b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

10. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

11. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

12. Before allowing any Subprocessor to Process any Personal Data related to the Framework Contract, the Processor must:

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Schedule 20 such that they apply to the Subprocessor; and

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

13. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

14. The Buyer may, at any time on not less than 30 Working Days' notice, revise this Schedule 20 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Framework Contract).

15. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Buyer may on not less than 30 Working Days' notice to the Supplier amend the Framework Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Where the Parties are Joint Controllers of Personal Data

16. In the event that the Parties are Joint Controllers in respect of Personal Data under the Framework Contract, the Parties shall implement paragraphs that are necessary to comply with GDPR Article 26 based on the terms set out in Annex 2 to this Schedule 20 (*Processing Data*).

Independent Controllers of Personal Data

17. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

18. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 of this Schedule 20 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

20. The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Framework Contract.

21. The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the Framework Contract;

(b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and

(c) where it has recorded it in Annex 1 *(Processing Personal Data).*

22. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

23. A Party Processing Personal Data for the purposes of the Framework Contract shall maintain a record of its Processing activities in accordance with Article 30 GDPR and shall make the record available to the other Party upon reasonable request.

24. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Framework Contract **("Request Recipient")**:

(a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

(b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

(i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

(ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

25. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Framework Contract and shall:

(a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

(b) implement any measures necessary to restore the security of any compromised Personal Data;

(c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

(d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

26. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Framework Contract as specified in Annex 1 *(Processing Personal Data).*

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

27. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Framework Contract which is specified in Annex 1 *(Processing Personal Data)*.

28. Notwithstanding the general application of paragraphs 2 to 15 of this Schedule 20 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs16 to 27 of this Schedule 20.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Annex 1 - Processing Personal Data

This Annex will be completed for each work order call off and is included in schedule 6 of the work order call off process.

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

1.1 The contact details of the Buyer's Data Protection Officer are: **Geoff Thompson geoff.thompson@food.gov.uk**

1.2 The contact details of the Supplier's Data Protection Officer are: **[Insert** Contact details]

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: • ***[Insert** the scope of Personal Data which the purposes and means of the Processing by the Supplier is determined by the Buyer]* **The Supplier is Controller and the Buyer is Processor** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data: • ***[Insert** the scope of Personal Data which the purposes and means of the Processing by the Buyer is determined by the Supplier]* **The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	• ***[Insert** the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together]* **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: • *Business contact details of Supplier Personnel for which the Supplier is the Controller,* • *Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Framework Contract) for which the Buyer is the Controller,* • ***[Insert** the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Buyer cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Buyer]* **[Guidance** where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified]
Duration of the Processing	***[INSERT** Clearly set out the duration of the Processing including dates]*
Nature and purposes of the Processing	***[INSERT** Please be as specific as possible, but make sure that you cover all intended purposes.* *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*

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

	combination, restriction, erasure or destruction of data (whether or not by automated means) etc. *The purpose might include: employment processing, statutory obligation, recruitment assessment etc]*
Type of Personal Data	***[INSERT** Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*
Categories of Data Subject	***[INSERT** Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]*
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	***[INSERT** Describe how long the data will be retained for, how it be returned or destroyed]*

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Annex 2 - Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Schedule 20 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 of Schedule 20 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Buyer]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

(b) shall direct Data Subjects to its 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;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Buyer's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Buyer each undertake that they shall:

(a) report to the other Party every [x] months on:

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

(i) the volume of Data Subject Access Request (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 Legislation;

(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 subject matter of the Framework Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) 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 the Framework Contract or is required by Law). For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

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

(f) 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;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

(g) 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 Annex 2 (Joint Controller 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 the 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 Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

(i) nature of the data to be protected;

(i) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, 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 as soon as it becomes aware of a Personal Data Breach.

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

3. Data Protection Breach

3.1 Without prejudice to Clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the Buyer and its advisors with:

(a) 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 Legislation;

(b) all reasonable assistance, including:

(i) 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;

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

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

(iv) providing the other Party and to the extent instructed 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 3.2.

3.2 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 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 of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

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

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

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

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

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

4. Audit

4.1 The Supplier shall permit:

(a) the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the Framework Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Framework Contract, in accordance with the terms of Article 30 GDPR.

6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Framework Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

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

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach 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 the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (*Resolving disputes*).

7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("**Court**") 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 the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

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

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Buyer shall be entitled to terminate the Framework Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the Framework Contract*).

9. Sub-Processing

10.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Framework Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

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 necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the Party for statutory compliance purposes or as otherwise required by the Framework Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Schedule 21 (Variation Form)

This form is to be used in order to change the Framework Contract in accordance with Clause 24 of the Core Terms (Changing the Framework Contract)

Framework Contract Details	
This variation is between:	**[**Buyer**]** (**"the Buyer"**) And **[insert** name of Supplier**]** (**"the Supplier"**)
Framework Contract name:	**[insert** name of Framework Contract to be changed] **("the Framework Contract")**
Framework Contract reference number:	**[insert** Framework Contract reference number]
Details of Proposed Variation	
Variation initiated by:	**[delete** as applicable: Buyer/Supplier]
Variation number:	**[insert** variation number]
Date variation is raised:	**[insert** date]
Proposed variation	
Reason for the variation:	**[insert** reason]
An Impact Assessment shall be provided within:	**[insert** number] days
Impact of Variation	
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]
Outcome of Variation	
Framework Contract variation:	This Framework Contract detailed above is varied as follows: • **[Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

1. This Variation must be agreed and signed by both Parties to the Framework Contract and shall only be effective from the date it is signed by the Buyer
2. Words and expressions in this Variation shall have the meanings given to them in the Framework Contract.
3. The Framework Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Buyer

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature .....

Date .....

Name (in Capitals) .....

Address .....

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

Schedule 22 (Insurance Requirements)

1. The insurance you need to have

1.1 The Supplier shall take out and maintain or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than

the Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

1.2.4 maintained for at least six (6) years after the End Date.

1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Buyer shall be indemnified in respect of claims made against the Buyer in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

2.1 Without limiting the other provisions of this Framework Contract, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

3. What happens if you aren't insured

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Buyer may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance you must provide

4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Buyer, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. Making sure you are insured to the required amount

5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Framework Contract and if any claims are made which do not relate to this Framework Contract then the Supplier shall notify the Buyer and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

6.1 The Supplier shall notify the Buyer in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Buyer (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or the Framework Contract for which it may be entitled to claim under any of the Insurances. In the event that the Buyer receives a claim relating to or arising out of the Framework Contract or the Deliverables,

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

the Supplier shall co-operate with the Buyer and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

7.2 Except where the Buyer is the claimant party, the Supplier shall give the Buyer notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Framework Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Buyer) full details of the incident giving rise to the claim.

7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Buyer any sum paid by way of excess or deductible under the Insurances whether under the terms of this Framework Contract or otherwise.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following insurance cover from the Start Date in accordance with this Schedule:

1.1 professional indemnity insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than] five million pounds (£5,000,000);

1.2 public liability insurance [with cover (for a single event or a series of related events and in the aggregate)] of not less than five million pounds (£5,000,000); and

1.3 employers' liability insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

1.4 product liability insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

Schedule 27 (Key Subcontractors)

1. Restrictions on certain subcontractors

1.1 The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Award Form.

1.2 The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.

1.3 Where during the Framework Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of the Buyer and the Supplier shall, at the time of requesting such consent, provide the Buyer with the information detailed in Paragraph 1.4. The decision of the Buyer to consent or not will not be unreasonably withheld or delayed. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Award Form. The Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;

1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

1.3.3 the proposed Key Subcontractor employs unfit persons.

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

1.4 The Supplier shall provide the Buyer with the following information in respect of the proposed Key Subcontractor:

1.4.1 the proposed Key Subcontractor's name, registered office and company registration number;

1.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;

1.4.3 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the Buyer that the proposed Key Sub-Contract has been agreed on "arm's-length" terms;

1.4.4 the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Framework Contract Period; and

1.4.5 (where applicable) Credit Rating Threshold (as defined in Schedule 24 (Financial Distress)) of the Key Subcontractor.

1.5 If requested by the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.3, the Supplier shall also provide:

1.5.1 a copy of the proposed Key Sub-Contract; and

1.5.2 any further information reasonably requested by the Buyer.

1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:

1.6.1 provisions which will enable the Supplier to discharge its obligations under the Framework Contract;

1.6.2 a right under CRTPA for the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon the Buyer;

1.6.3 a provision enabling the Buyer to enforce the Key Sub-Contract as if it were the Supplier;

1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to the Buyer;

1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:

(a) the data protection requirements set out in Clause 14 (Data protection);

(b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);

(c) the obligation not to embarrass the Buyer or otherwise bring the Buyer into disrepute;

DocuSign Envelope ID: 65C38BA1-57C0-4E75-B800-B7102EDBF8C8

(d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and

(e) the conduct of audits set out in Clause 6 (Record keeping and reporting);

1.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on the Buyer under Clauses 10.4 (When the Buyer can end this Framework Contract) and 10.5 (What happens if the Framework Contract ends) of this Framework Contract; and

1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of the Buyer.