Award Form

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: IntaForensics Limited Address: 9, The Courtyard, Eliot Business Park, Nuneaton, CV10 7RJ Registration number: [05292275] 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:

	(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

		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**	[**Sam Walton**] [**Sales Operations Manager**] [**Sam.Walton@intaforensics.com**] **[02477 717 780**]
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

Signed for and on behalf of the **Supplier**	Signed for and on behalf of the **Buyer**
Name: [**Andrew Frowen**] **[Chief Executive Officer]**	Name: [**Caroline** Terry Commercial Business Partner
Date: 18/11/2020	Date: 02/12/2020
Signature:	Signature: Terry

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.

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
- 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 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.

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
- 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
- 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
- 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.

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
- 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

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
- 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

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).

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:

- 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
- 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.

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

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
- 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.

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

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:

- 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.

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
- 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.

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.

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:

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:

"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; 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;
"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;
"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 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
"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, 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;
"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: 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;
"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;
"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 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 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 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 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;
"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: 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;
"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;
"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; 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 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;
"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;

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.

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.
- 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
- 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
		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:

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?

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;

   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;

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

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	FS900084
Tender Title	Digital Forensic Provider Framework
Full legal organisation name	IntaForensics Limited
Main contact title	Mr
Main contact forname	Andrew
Main contact surname	Frowen
Main contact position	CEO
Main contact email	Andrew.frowen@intaforensics.com
Main contact phone	02477 717 780
Will you charge the Agency VAT on this proposal?	Yes
Please state your VAT registration number:	GB 900353372

Project Costs Summary Breakdown by Participating Organisations

Please include only the cost to the FSA.

Organisation	VAT Code*	Total (£)
IntaForensics Limited	STD	£ 37,650.00
Total Project Costs (excluding VAT) **		**£ 37,650.00**

* 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.

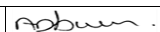
Project Costs Summary (*Automatically calculated*)

Staff Costs	**£**	**36,640.00**
Overhead Costs	**£**	**-**
Consumables and Other Costs	**£**	**110.00**
Travel and Subsistence Costs	**£**	**900.00**
Other Costs - Part 1	**£**	**-**
Other Costs - Part 2	**£**	**-**
Other Costs - Part 3	**£**	**-**
Other Costs - Part 4	**£**	**-**
Other Costs - Part 5	**£**	**-**
Total Project Costs	**£**	**37,650.00**

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:

IntaForensics Ltd offer their public sector customers a scaled annualised spend rebate. This is detailed as follows:
Annual spend up to £250k = 2.5%
Annual spend between £251k and £500k = 5%
Annual spend over £501k = 10%

SIGNATURE		
NAME	Andrew Frowen	
DATE	22-Jul-2020	
REVISION DATE	22-Jul-2020	Enter the effective date if this version of the template replaces an earlier version

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)
SPOC - PM & Review Manager	IntaForensics Ltd	£ 1,000.00		23	£ 23,000.00
Forensic Operations Manager	IntaForensics Ltd	£ 800.00		2	£ 1,600.00
Principal Experts	IntaForensics Ltd	£ 800.00		6	£ 4,800.00
Forensic Analysts	IntaForensics Ltd	£ 680.00		9	£ 6,120.00
Forensic Processing Team	IntaForensics Ltd	£ 560.00		2	£ 1,120.00
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -
					£ -

Total Labour Costs	**£ 36,640.00**
* Total Overhead Costs (if not shown above)	

Food Standards Agency
food.gov.uk

Consumable/Equipment Costs

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

Item	Quantity	Cost/Item(£)	Total
Data Storage 2TB Drives	2	£ 55.00	£ 110.00
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -

Total Material Costs	**£ 110.00**

Please provide, in the table below, estimates of other costs that do not fit within any other cost headings

	Description and justification of the cost	Estimated Cost
1		£ -

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
Meal Allowance for onsite operation	6	£ 25.00	£ 150.00
Overnight accommodation if required	6	£ 125.00	£ 750.00
Travel (included in day rate)		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -
		£ -	£ -

Total Travel and Subsistence Costs	£ 900.00

Rate Card

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

Role or position	Maximum Hourly Rate	Maximum Daily Rate	Daily Overhead rate
SPOC, Project and Data Review Manager	£ 125.00	£ 1,000.00	##########
Forensic Ops Manager	£ 100.00	£ 800.00	£ 80,000.00
Principal Expert	£ 100.00	£ 800.00	£ 80,000.00
Forensic Analyst	£ 85.00	£ 680.00	£ 57,800.00
Forensic Processing Team	£ 70.00	£ 560.00	£ 39,200.00
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -
	£ -	£ -	£ -

Schedule 4 (Tender)

Lead Applicant's details							
Surname	Frowen	First Name	Andrew	Initial	D	Title	Mr
Organisation	IntaForensics Limited	Department	Board Director/CEO				
Street Address	9, The Courtyard, Eliot Business Park						
Town/City	Nuneaton	Country	United Kingdom	Postcode	CV10 7RJ		
Telephone No	02477 717 780	E-mail Address	andrew.frowen@intaforensics.com				

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

TENDER SUMMARY			
Digital Forensic Provider Framework			
	01/09/2020		01/09/2022

1: delivery of the requirements For THe FRAMEWORK AGREEMENT

A. TENDER SUMMARY

IntaForensics Limited is responding to an invitation to tender which will see a framework established for Digital Forensic Service Providers. The service that will be delivered on this framework will involve IntaForensics supporting the FSA National Food Crime Unit (NFCU) with criminal investigations by forensically capturing digital evidence from locations across England and Wales, securely transporting the data and undertaking preliminary analysis. The accredited processes (ISO/IEC 17025) implemented by IntaForensics' experts will ensure that the NFCU can conduct further analysis and produce evidence in court to support their criminal investigations.

For the majority of requests, IntaForensics envisage being provided 72-hours' notice by the NFCU to support a warrant/search and seize operation. Crime scenes and locations are likely to comprise a variety of descriptions such as meat processing factories, commercial premises and private dwellings. IntaForensics will provide skilled and experienced digital investigation and examination experts to support NFCU investigators whilst on-

scene. These experts can capture and preserve data from complex and large IT systems such as servers, as well as data from satellite navigation systems and personal digital devices. Staff will conduct forensic imaging on digital media found at the scenes in the first instance, however in some circumstances it may be required that IntaForensics seize the digital media. Should the capture of data from printing or labelling machines not be possible, IntaForensics will liaise with relevant manufacturers to produce evidential products for the NFCU. The services provided will include securely transporting the collected data or the seized exhibits back to IntaForensics' accredited and secure forensic laboratory.

Where required, IntaForensics will conduct analysis on the collected data or exhibits at a securely accredited facility in line with the forensic strategy, all work conducted will comply with the Criminal Procedure and Investigation Act (CPIA) 1996. Analysis will include keyword searches on information provided by NFCU investigators to identify material of relevance to the investigation. Due to the nature of such investigations, it is highly likely that Legal Professional Privilege (LPP) material will be identified and generated; in such instances, IntaForensics will separate this material to ensure that independent counsel can review. At the conclusion of the analysis, a technical report and witness statement will be provided to the NFCU, additionally, a review package will be provided on a reviewing platform to enable NFCU investigators to work on the same investigation in multiple locations and review all relevant information remotely.

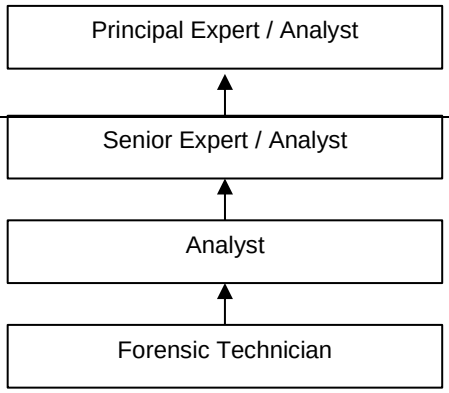
B. Named Staff Members who will work on THE FRAMEWORK and Details of their Specialism and expertise	
For each participating organisation on the project team please list:- the names and grades of all staff who will work on the project together with details of their specialism and expertise, their role 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	IntaForensics Limited
Named staff members, details of specialism and expertise.	

At the current time, IntaForensics has over 30 technical and analytical staff of various backgrounds and experience levels, located at the head office in Warwickshire. The expert team is comprised of:

- Mobile phone analysts
- Computer analysts
- Dual-trained analysts (analysis of both mobile phones and computers)
- Cell site (RFPS) experts
- Digital and social media investigators (DMI's)
- Dedicated pre-imagers and Imagers
- Incident response specialists
- Qualified Security Assessors (QSA)
- PCI Forensic Investigators (PFI's)

Due to capacity planning and operations/investigations across all client commitments, it is not possible at this time to confirm which analysts will be working on this framework. Dependent upon the requirement from the FSA NFCU, it is likely that some investigations will require 1 or 2 experts, whereas larger investigations will require up to 8-10 experts across both mobile and computer forensic fields.

The Digital Forensic and Cyber Security team are organised in a hierarchical structure, demonstrated below:



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.
IntaForensics currently provide short notice and out of office hours services to their customer base under managed contracts. As a long standing and current provider to the National Crime Agency (NCA), IntaForensics has supported the execution of many large operations and the delivery of ad-hoc onsite examinations and triage at both witness and suspect addresses including business premises. Additionally, IntaForensics recently worked with another regulatory UK body, the Competition and Markets Authority (CMA) for a second occasion, on a large onsite project, whereby IntaForensics analysts were deployed to assist officers in the coordinated execution of search warrants at multiple business premises located across the UK. **Evidence One** October 2014 – Ongoing (renewal date 2023) National Crime Agency £2,000,000.00 +

IntaForensics secured this contract with the NCA in both 2014 and 2019 respectively. This contract covers all aspects of digital forensic examination of all classes and types of digital device, including the provision of on-site support for NCA teams executing search warrants and the delivery of cell site analytics. During the first 4-year contract, IntaForensics provided the NCA with unrivalled digital forensic services and played a vital role in several large and confidential operations that were carried out nationally. For the second contract, awarded in 2019, IntaForensics were one of three suppliers selected due to our extensive scope of ISO/IEC 17025:2017 accreditation and technical capabilities, as demonstrated during the first contract. This contract is also a framework, available for regional forces and government agencies to utilise. IntaForensics currently also deliver services under this contract to Greater Manchester Police and West Midlands Police.

A large number of major operations conducted by the NCA have required onsite support at the crime scene, requiring a combination of triage or provision of need expert advice. IntaForensics have frequently been able to supply staff often with just a few hours' notice. At the time of writing, the company has supported the NCA in over 100 onsite operations involving various crime types (fraud, IIOC, drugs) requiring investigation of various complexities of IT infrastructures.

A specific operation was conducted in South Wales, involving the NCA and local officers with IntaForensics deploying multiple analysts to the scene. 48 hours notice was provided to IntaForensics from the NCA to provide technical support. Once onsite, the NCA officers made entry to the property and upon confirmation that the scene was secure, the analysts were given the authorisation to enter and search for digital media. A number of devices were located and were imaged in situ, these devices included mobiles and computers. A significant number of indecent images were located on the devices, alongside physical items in the property which were determined to be significant evidential items. Due to the rapid deployment of the IntaForensics team and the rapid turnaround of the initial examination – further grooming activity was identified. Based upon the evidence obtained by the team a suspect was arrested in the USA and is now serving a custodial sentence. A further 23 suspects were identified worldwide as part of this operation.

Many of IntaForensics' staff have existing, widespread experience of working alongside the NCA and other agencies in onsite operations, or have experienced similar operations in their previous employment, mostly with law enforcement or other commercial digital forensic laboratories. This means they can call upon their experience and skillset when encountering future requirements for onsite data capture and analysis.

Evidence Two

2017 and 2019 (Individual Operations)

Competition and Markets Authority (CMA)

Circa. £70,000.00

IntaForensics has twice been awarded large operations with the Competition and Markets Authority (CMA) for onsite projects. The first operation took place in 2017 where a total of 16 (sixteen) analysts were

simultaneously deployed to 8 (eight) locations across the UK. The project was originally planned to take place over 2 days, however due to significant quantities of digital media devices being discovered, the onsite and subsequent analysis work required the analysts to remain on scene for a further day. During the first project, analysts supported the investigation by conducting acquisitions of various devices including mobile phones, tablets, workstations, laptops, servers, USB's and memory cards. Experienced analysts facilitated the smooth delivery of the project as an in-depth understanding of the methods to extract data from the devices proved to be vital. The second and most recent operation took place in 2019 and involved 16 (sixteen) analysts being deployed to 8 (eight) locations across London and the rest of the UK. For both operations, the client was assigned a Single Point of Contact (SPoC) for all operational requirements. This meant that all communications and briefings were channeled through the Principal Expert to ensure the requirements were clear and that all sub teams were fully briefed and prepared.

Evidence Three

September 2018 – November 2019

Redacted customer name due to PFI guidelines and NDA confidentiality

Global Airline Company

Circa £400,000.00

As a Payment Card Industry Forensic Investigation company (PFI) and only 1 of 23 in the world accredited to perform forensic investigations data breaches involving payment card holder data, IntaForensics was engaged by a Global Airline Company in 2018 to respond and investigate a data breach that involved a significant number of card details. After completing the initial engagement it was clear that the environment was substantial and complex; therefore, a detailed scoping meeting was arranged and a dedicated team of cyber security analysts deployed to the customers site to perform the scoping project with the goal of identifying and determining the in-scope systems and environments for the required investigation. It was identified that there were over 150 systems in the environment that required investigation, this included in excess of 140 servers and more than 10 workstations which were located in 2 secure data centres.

The team gathered key information from the client and established that the servers were a mixture of Windows based systems and Linux. The workstations were confirmed to be Windows machines and were scheduled to be imaged in a secondary phase to the servers. The investigators were dispatched to the data centres in teams and began to image the servers using a mixture of FTK Imager for the Windows servers and a bespoke tool that the PFI team use specifically for Linux based systems. Once the image files and data were extracted, the data was securely transported to IntaForensics' secure laboratory to be analysed and reviewed using a variety of forensic tools including EnCase, X-Ways and others. The team ran multiple malware scans and tools across the datasets to identify indicators of compromise or for unauthorised applications. A detailed and full investigation was completed with in-depth reporting submitted to all stakeholders including the major card schemes and acquiring banks. Throughout the complex investigation, regular update meetings were hosted by the PFI team to provide vital updates as the investigation progressed.

Additional Evidence

After a competitive tender process, IntaForensics was awarded a contract with the Information Commissioners Office (ICO) for the provision of digital forensic services, with the majority of this work involving urgent on scene attendances. Due to the current worldwide circumstances, the timing of this contract has meant that no on-scene attendances have been conducted at the time of writing. Drafting of Service Level Agreements is currently in progress, with the aim to have these completed shortly, this will allow the expert team to respond to requests for support.

IntaForensics also provide incident response services to a number of retained clients and new customers, with the majority of incidents requiring same day or next day deployments. The team have frequently responded out of hours to contain incidents with the commencement of a digital forensic investigation taking place within hours of the first call for assistance.

Due to the urgent or short notice nature of these requests, IntaForensics frequently receives notification of an operation with only minimal notice and the necessary arrangements must be made to dispatch an expert, often on the same day if required. This requires all experts to respond dynamically, often with no indication as to the number or type of exhibits that may need seizing, triaging or analysing. The company's comprehensive expertise with regular projects such as this enables the analysts to overcome difficult challenges with professionalism, integrity and ease. Up to eight (8) analysts can also be placed on 'standby' should there be a need for additional urgent resource at sites of collection. IntaForensics maintains a number of comprehensive 'field kits' for immediate deployment containing both validated forensic tools and hardware necessary for onsite triage and acquisition of mobile and computing devices in such cases.

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 Assurance 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 internationally accepted quality standards specified in the ITT e.g. ISO 9001 and ISO17025.

IntaForensics proudly hold a comprehensive scope of accreditation to ISO/IEC 17025:2017 in accordance with the requirements of the Forensic Science Regulator (FSR). IntaForensics is also accredited to the FSR Codes of Practice and Conduct, in addition to being certified to ISO 9001:2015, ISO/IEC 27001:2013, ISO 14001:2015 and Cyber Essentials Plus.

IntaForensics has achieved and maintained a comprehensive scope of accreditation for ISO/IEC 17025:2017 to cover:

Mobile Device: Dual tool scope for both the physical and logical capture and preservation of data and processing of data (SIM Card, handset and tablets) using Cellebrite UFED and MSAB XRY
Computer and Digital Storage Devices: Physical capture and preservation of data (Forensic Copy) using EnCase, FTK Imager, MacQuisition and CAINE (Guymager)
Computer and Digital Storage Devices: Processing and analysis of data from digital media for MS Windows and Apple operating systems using EnCase and Internet Evidence Finder (IEF), Griffeye with Blue Bear and LACE Carver
Satellite Navigation Systems: Physical and logical capture and preservation of data from Sat Nav systems using FTK Imager and in-house manual extraction methods
Drones (Unmanned Aerial Vehicle) – DJI, Parrot: Physical and logical capture and preservation of data, logical capture and processing of data using MSAB XRY, MSAB XAMN, Cellebrite UFED 4PC and Cellebrite UFED Physical Analyser.
The current Extension to Scope for the use of both AXIOM and BlackLight in processing and analysis of data from digital devices has been scheduled for October 2020 for UKAS assessment.

A further Extension to Scope has been completed for Cell Site analysis detailing the area of testing, the type of test and range of measurement and also the specific forensic tools and equipment used, with IntaForensics being an active member of the current UKAS pilot scheme for cell site accreditation.

The Forensic Science Regulators (FSR) Code of Practice and Conduct to cover ALL practices under our ISO/IEC 17025 scope of accreditation.

In addition to our ISO/IEC 17025:2017 accreditation, IntaForensics has made an application to UKAS for accreditation relating to search, identification, recovery, recording, selecting, examination and interpretation of digital devices from scenes of crime for forensic purposes under ISO/IEC 17020:2012. This is referenced under UKAS project number 304827 and, at the time of writing, IntaForensics are the first digital forensic applicant for this accreditation to be received by UKAS. Due to the ongoing pandemic we anticipate the UKAS assessment will not take place before November 2020.

IntaForensics operates an integrated Quality Management System that meets the requirements of all our accreditations and certifications. This includes certification to ISO 9001:2015, which certifies the core management system and ensures that the company delivers services that meet customer requirements.

IntaForensics certification to ISO/IEC 27001:2013 demonstrates information security management and the effective use of control measures in securing business operations.

The company's certification against ISO 14001:2015 demonstrates commitment to sustainability and the environment and is detailed below in Section B.

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)

As evidence of IntaForensics' commitment to the environment and sustainable working methods, the company has achieved certification to ISO 14001:2015. All staff recognise and accept their responsibilities around managing the environmental impacts of the business and the company has put in place controls for business activities that may influence the environment. An Environmental Policy is in place at the company (IF-SOP-37) and addresses the main responsibilities including:

- Controlling operational activities with a view to identifying cost savings through improved efficiency and productivity
- Reduction of energy use and waste
- Controlling reputational risk by demonstrating the commitment to protecting the environment
- Bring reputational advantages and enhancing the public image
- Demonstrate a future-focused organisation that aims to reduce their carbon footprint

The company regularly evaluates the environmental impact of its activities, products and services and will act to continually improve the environmental performance of the organisation.

It is the company's mission to:

- Minimise the use of energy, water and natural resources
- Minimise waste through prevention, re-use and recycling where possible
- Dispose of waste safely and legally
- Avoid the use of hazardous materials, where practicable
- Work with environmentally responsible suppliers
- Prevent environmental damage and minimise nuisance factors such as noise and air pollution

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 Specification 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.

Applicants are reminded that, where appropriate, the need to obtain clearance for the proposed project from their local ethics committee. This 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.
IntaForensics has identified the acquisition of personal data to potentially be an ethical issue. Data Protection is an important ethical issue, not only in research projects but also in an investigation context, additionally protection of such information is a legislative and fundamental human right. Whilst IntaForensics do not envisage conducting research activities, it is foreseeable that personal data may be extracted as part of any digital data investigation, requiring that all processes and procedures must demonstrate compliance with GDPR. The Company's Data Protection and GDPR policy (IF-SOP-20) fully details how personal data is acquired, handled and securely disposed of. Robust mechanisms are in place for the management of any Subject Access Requests (SAR) with details of how these can be made, published on the Company website. IntaForensics has not identified any other ethical issues with this project.
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 raised 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 information 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 between 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/archive) and/or procedures for the destruction of physical and system data should also be included in this part (this is particularly relevant for survey data and personal data collected from clinical research trials). The project Lead Applicant will be responsible for ensuring that they and any sub-contractor who processes or handles information on behalf of the FSA are conducted securely.
Data Protection issues IntaForensics would assert that Legal Professional Privilege (LPP) is a specific potential data protection issue with this project. LPP is a fundamental legal right and a powerful tool under English Law, granting individuals and corporate entities the right to resist disclosure of confidential and potentially sensitive material in the context of arbitration, litigation and investigations. IntaForensics has extensive involvement in criminal and civil law investigations across the UK on a regular basis and acknowledge the significant importance of this

issue. To ensure that IntaForensics' analysts approach this material in a sensitive and legal way, a Standard Operating Procedure (SOP) was issued and forms part of the accreditation Quality Management System.

A copy of the Legal Professional Privilege Policy is attached as part of this response.

Data Protection Processes and Systems

As an IASME accredited Certification Body for Cyber Essentials and Cyber Essentials Plus, IntaForensics is fully aware of the requirements of GDPR and other relevant Data Protection legislation, such as the Data Protection Act 2018 (which complements the European Union's General Data Protection Regulation and has updated the Data Protection Act 1998).

Ongoing compliance with the company's numerous accreditations (ISO 27001 and the FSR Codes of Practice and Conduct) ensure that all systems are designed and operated as to ensure the security of all assets, physical and intellectual. The company's Data Protection and GDPR policy (IF-SOP-20) fully details how personal data is acquired, handled and securely disposed of. Robust mechanisms are in place for the management of any Subject Access Requests (SAR) with details of how these can be made, published on the Company website.

As a virtually paper-free organisation, the vast majority of both client and employee personal information is recorded and stored securely within the case management system Lima. Any information not within Lima is securely stored on encrypted internal networks with access granted on a least privilege basis.

IntaForensics ensures that all seized equipment and exhibits are securely held by designing processes, policies and procedures with the aim of safeguarding all exhibits, evidential data and output in line with best practice and full accountability. IntaForensics holds and has maintained ISO 27001 for many years; this is underpinned by a comprehensive Information Security Management System, which is annually audited and verified. In addition, the company engages a third party to conduct penetration tests of the IT network on at least an annual basis.

All processes relating to data, physical exhibits and other evidential material are covered as part of the company's holistic and layered approach to security. This is to ensure that security is designed and plays a core role in all activities undertaken; from the recruitment through to the handling of physical exhibits and evidential data files, full chain of custody management, encryption protocols for evidential output and data in transit and at rest as well as all other aspects of the operation.

Physical Infrastructure

IntaForensics laboratory is located within a secure courtyard surrounded by a 2m high fence line with singular vehicle access by proximity-controlled gates. Access to the courtyard is restricted and controlled and an external security company conducts visible external patrols of the site. The building itself is equipped with a Red Care Alarm System that is monitored 24/7 and is responded to by the Police and an external security company. In addition, a high quality digitally recorded CCTV system covers internal operationally sensitive areas in addition to external coverage.

Access to exhibits in the secure laboratory is controlled by physical means, complimented by encryption on stored materials. Physical measures include secure access control across multiple access points before reaching the exhibits store. IntaForensics' laboratory has been assessed by both the Metropolitan Police Service and the National Crime Agency to ensure that the physical and IT infrastructure meets their stringent security requirements. Both the Cyber and Forensic Laboratories located in the building are security grille protected and have privacy film to the windows, the secure exhibits store also has these protective features.

Custody of Physical Exhibits

Collected exhibits are transported non-stop in IntaForensics' own unmarked, GPS tracked vehicles which are staffed by IntaForensics security vetted employees. Where security or operational needs arise, the vehicle will have two staff on-board. Exhibits imaged during on-scene attendance will have the forensic images and data stored directly onto encrypted forensic hard disks – preventing any unauthorised access to the data whilst it is in transit from the scene back to the secure forensic laboratory.

Upon arrival at the laboratory, trained staff will complete the collection record and assign the exhibits to a uniquely referenced location in the secure exhibits store. This store is proximity access controlled and is only accessible to operational staff. All evidential materials are stored in the secure exhibit storage with all interactions with the exhibit or forensic image recorded within IntaForensics' Lima Case Management system. This system allows IntaForensics to provide a full audit trail and ensure that there is a documented chain of custody. IntaForensics will assess the material being returned and provide an appropriate level of data encryption. This encryption methodology will be defined under the agreed the SLA. Passwords are never sent with the evidential package; these are communicated separately via the Criminal Justice Secure Messaging (CJSM) system or other secure means of communications as will be mutually agreed with the FSA and discussed during the contract mobilisation process.

At the conclusion of the case, whereby the physical exhibits are transferred back to the agreed point of contact, a full handover procedure is in place to capture a record of this transfer of custody. This will be in the form of an internally generated dispatch notification and enabling the recorded transfer of the custody of the exhibits and any generated materials back to the NFCU investigator.

Archives and Retention

IntaForensics confirms that all data is securely archived in accordance with the SLA for clients and is purged and/or destroyed in those situations in accordance with FSA instructions and standards. All operational staff at IntaForensics adhere to IF-SOP-18 (Case Archive Procedure) when archiving cases to ensure the generic process is clearly carried out. The process includes adding the archive entry onto Lima and, dependent on

specific client instructions, the staff member will then archive the case drive onto a tape ready to move into storage.

In the event of the instruction being received to securely wipe or delete the data, IntaForensics will follow LAB-SOP-09 (Hard Disk Wiping Procedure) and LAB-SOP-18 (Case Archive Procedure) Section 3.5 Destroying Archives; both SOP's can be provided upon request. All case related data derived from exhibits is stored on PDE encrypted Hard Drives or RAID arrays and analysed on a secure, encrypted standalone network infrastructure. IntaForensics will propose an exit strategy for data retention and this will be addressed in the mobilisation plan and agreed with the FSA contract team prior to service commencement.

IntaForensics can confirm that no sub-contractors will be used as part of this framework.

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.

The objective of this project is to implement a framework where call-off services (work packages) will be directly awarded to framework qualified suppliers. Upon award of a place on the framework, IntaForensics will seek to arrange a framework mobilisation meeting with the FSA where they will be invited to visit IntaForensics' secure and accredited forensic laboratory to create an agreed Service Level Agreement (SLA). SLA's are an extremely important part of working with IntaForensics as they define the agreed processes and communication contacts for the framework. Whilst IntaForensics acknowledge that individual call out services will require their own forensic strategy due to unique requirements, an overarching agreed SLA will ensure that timescales are met and standard processes are followed – ensuring a smooth and consistent approach when directing work to IntaForensics.

IntaForensics operate a customer-focused service and assign key account managers to all contractual clients, whether this be on a framework or on direct awards. With all accounts, IntaForensics aims to develop integrated and meaningful partnerships which provide:

- Deployment of innovation and the results of research & development to support long term economic delivery of services
- Engagement with supplier relationship management activities
- Co-ordinated communications with stakeholders within IntaForensics and the FSA
- Visibility and transparency across whole framework period

The account management team at IntaForensics has extensive experience of working with public sector clients including the NCA and Metropolitan Police Service (MPS) and have skillsets and experience in the following areas:

- Client relationship management
- Financial analysis and management
- Process and requirements analysis and management
- Dispute resolution and complaints
- Managing and handling digital forensic and cyber security projects of varying size
- Management information and reporting skills
- Quality improvement projects

When working with the Competitions and Markets Authority (CMA) in 2019 for on-scene attendance and imaging/pre-analysis requirements, IntaForensics provided the CMA investigation team with a Single Point of Contact (SPoC). This method has been proven to assist in the planning and logistical involvement of an investigation and certainly contributed to the smooth and successful running of the operation. IntaForensics will therefore seek to implement the SPoC method with the FSA for any call-off service requirements. The designated SPoC will ensure that the forensic strategy is followed and will be instrumental in planning and supporting the FSA with their requirement. All work requests from the FSA will be managed on the Lima Forensic Case Management System.

IntaForensics develop a world leading Forensic Case Management System (Lima), which was designed in 2006 and commercially released in 2009 across both law enforcement, Government agencies and commercial companies in both the UK and across the world. The system has been developed by digital forensic practitioners at IntaForensics and has been continuously updated and improved over 11 years using feedback and suggestions from the Lima user community.

The Lima system is utilised by all departments at IntaForensics, the Key Account Management team log work requests and track communications, the submissions and logistical teams use the system to schedule exhibit collections and deliveries and to track custody records of evidence, whilst the digital forensic and cyber investigation teams use Lima to manage cases, book in and out exhibits, log notes and timeline entries and then generate reports and statements. The system also allows IntaForensics accounts and management teams to compile Management Information (MI) reports for customers and critically manage capacity across the laboratory teams.

As part of the SLA with the FSA, an agreement will be made regarding the format of the analyst preparing their contemporaneous notes. IntaForensics can facilitate this in a number of ways, the first way will involve the analysts making a physical copy of their contemporaneous notes whilst on scene. In order to facilitate this, the analysts will note all their activity in writing in a dedicated notepad which will be supplied prior to the commencement of the project. Upon completion of their examination(s), the analyst will seal their notes in an evidence bag and exhibit this in their supporting MG11 s9 Witness Statement.

Alternatively, IntaForensics can use Lima Forensic Case Management to manage information obtained in the field as well as in the laboratory. Prior to being deployed in the field, the IntaForensics analyst can create a Lima ‘offline package’ which can then be used to log all activity any seized material and all contemporaneous notes that are made by the analyst during their deployment onsite. Once they return to the lab, the Lima case package can then be imported back, automatically populating the case log with data captured during the search warrants.

F. 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 be taken to minimise these risks and how they will be managed by the project team.

Please add more lines as required

Identified risk	**Likelihood of risk (high, medium, low)**	**Impact of Risk (high, medium, low)**	**Risk management strategy**
Digital devices found on scene differ to the ones expected to be encountered	Medium	Medium	All forensic onsite operations are planned to handle different types of media, such as mobile phones and computers. Forensic onsite kits carry a selection of imaging tools and can cater for both computer and mobile devices. In the event of more devices being discovered then this can impact the time on scene due to the size of the data being captured.
Evidence accessed during transit could result in a loss of confidentiality and case related data. This then impacts the chain of custody and will compromise the integrity of the data and exhibits.	Low	High	The IntaForensics Operations Management team ensure that this risk is managed by ensuring that strict exhibit continuity and chain of custody processes are in place, as well as having secure delivery vehicles (GPS tracked) and trained staff. Exhibits will be placed into sealed tamper evident transit bags and containers as well as a full track and trace process for all exhibits outside of IntaForensics premises. Drives will be encrypted for transit to ensure no unauthorised access is allowed.
Problems with software and forensic tools not functioning	Low	Medium	

correctly or as expected as per the vendors specification which can mean Information relevant to the case is not available for processing and analysis.			A robust validation programme is implemented at IntaForensics which involves testing and challenging the applications in operation within the laboratory. Isolated validation workstations constructed to reflect the operation are facilitated to identify any conflicting applications. Onsite kits are regularly checked and validated to ensure that the tools are problem free and up to date.
During an onsite activity, a number of risks are identified. These are: Potential loss of security. Exposure of assets Potential unauthorised access to data/information/equipment. Potential physical risks to staff.	Low	High	Operations Management tackle this risk by ensuring that onsite operations follow a structured deployment process which is carried out in accordance with instructions from the OIC (client). Dedicated equipment and onsite kits are prepared and ready for deployment when required. Documented processes and procedures are in place for onsite activity, IF-SOP-39.

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.
IntaForensics envisage that a direct award in the form of a work package will be sent to the IntaForensics Submissions Department, copying in the account manager responsible for FSA related operational requirements. The contact information and desired process will be agreed in a Service Level Agreement (SLA) which will be created and disseminated upon the award of a place on the framework. The Submissions team will then respond, confirming receipt and a case requirement will be created on the company's case management system (Lima). As part of the agreed SLA, IntaForensics will assign the case to a Principal or Senior expert for them to review the FSA's requirements and to produce a forensic strategy. The forensic strategy will detail the approach that IntaForensics seek to adopt and this will be based on the requirements in the work package. The forensic strategy will be sent to an agreed contact at the NFCU for review and approval. Once approval is received, the case is awarded and assigned to the Principal/Senior expert and they will begin their role as Single Point of Contact (SPoC). The SPoC will seek to organise a pre-deployment meeting with NFCU and operations management at IntaForensics, this meeting will identify the locations in scope of the operation, possible risks to on-scene attendance (warehouses, corporate building and meat processing factories) and an early indication of possible devices that will be encountered. A detailed strategy with additions and suggestions from NFCU will be complied and circulated to all involved within 72 hours of the initial work package being received by IntaForensics. The SPoC will attach the strategy to the Lima case and assign all required analysts to ensure that they will be updated with any comments on the case and also provide them with quick and easy access to the required materials before deployment. As the scenario details 3 (three) locations in total; HQ, Location 1 and Location 2, IntaForensics will deploy a minimum of 2 (two) analysts to each location, totalling 6 (six) onsite analysts for this operation – designated sub teams. The SPoC, an escalation point of contact as well as additional computer support and the IntaForensics processing team will be briefed on the operation and all placed on standby at the secure forensic laboratory. During the pre-deployment meeting, IntaForensics will provide a number of approaches for NCFU sign off before these are conducted onsite. Considerations will also be provided to the classification of exhibits, for example: • Vital – Exhibit will be subject to thorough examination regardless and as such does not require triage. This may be due to circumstances or information known that clearly identifies that this exhibit is likely to contain key evidence • Triage – Triage devices will be subject to keyword searches and the results interpreted and fed back for a decision on whether to proceed with further analysis • Possible – Exhibits that are not considered vital at that moment but can be imaged and retained to progress to triage as and when required Once an agreement has been reached on approaches, timeframes and resources, the team will conduct pre onsite checks, which include ensuring that the onsite kits are reviewed and prepared, ready for the onsite date. All communications and updates will be fed through the SPoC who will be responsible for updating the Lima case details. The SPoC will chair an internal meeting with all involved analysts and support staff which will cover in detail the expectations, requirements and role allocation. Each sub team will be provided with their location and advised on the NFCU investigator they will accompany and what potential digital devices they may be encountering. IntaForensics' IF-SOP-39 - Onsite Forensic Activity Procedure provides all IntaForensics staff with guidance and covers the processes that are applied when attending a scene for the execution of search

warrants and acquiring data from devices of all types including servers and live data, seizing exhibits, triage processes and evidence handling. These processes are in line with ISO/IEC 17020 standards which cover on-scene attendance; a brief summary is provided below.

Ensuring correct on-site forensic imaging equipment is available for mobile phones, computer systems and live data.

The following forensic tools would typically be considered:

- Cellebrite UFED
- MSAB XRY
- BlackBag Technologies MacQuisition
- AccessData FTK Imager
- Guidance Software Tableau Forensic Duplicator (TD2/U)
- CAINE
- Guymager

All the forensic tools listed above are covered in the company's extensive ISO/IEC 17025 scope of accreditation, validated and/or calibrated regularly and asset tracked via IntaForensics' case management system (Lima). In addition to our ISO/IEC 17025:2017 accreditation, IntaForensics has made an application to UKAS for accreditation relating to search, identification, recovery, recording, selecting, examination and interpretation of digital devices from scenes of crime for forensic purposes under ISO/IEC 17020:2012. This is referenced under UKAS project number 304827 and, at the time of writing, IntaForensics are the first digital forensic applicant for this accreditation to be received by UKAS. Due to the ongoing pandemic we anticipate the UKAS assessment will not take place before November 2020.

Upon deploying to the locations, the teams will seek to use the following tools and approaches for each of the devices on scene:

Location 1 and Location 2

The servers at these locations will be imaged using FTK as they are Windows-based servers, however the team will arrive with secondary software in case of any unforeseen issues with the imaging of the data. The size of the data will allow the sub team to be able to acquire the data on multiple hardware encrypted USB devices, this would require the servers to have a USB output. If USB 2.0 output is in place, the teams will still be able to acquire the data in a reasonable time frame Verification of the acquired images would be taken on site to ensure that a sound image has been taken before leaving site. Depending on the requirements from NCFU, the sub teams may be able to keep the servers in situ for continuation of company business as opposed to taking these offline to take a forensic image. If the servers can be taken offline, the team will seek to acquire the data from the hard drives using a Tableau Writeblocker to ensure a forensic data acquisition onto encrypted hard drives.

HQ Location

The sub-team consisting of 2 (two) Principal experts will deploy to the headquarters of the company. They will arrive on-scene with the prepared equipment and will commence their imaging of the file server and email server. The email server can be imaged on site which will require the cloning of the hard drives; depending on the size of the data this could take most of the morning to facilitate. Another option that will be discussed during the pre-meeting is whether the NCFU are focused on specific users, if that is the case, the team will conduct a live PST file export of the Exchange server for each user. Admin credentials will need to be provided to ensure access to the live server. The PST files will be hashed and preserved as logical EnCase files (LEF). The live access method is quicker and will also reduce any potential client concerns of collateral intrusion. The file server would be a simple live image process on site and a standard image will be obtained and taken back to the forensic laboratory.

Seized Devices

The digital media devices recovered from the company directors will be seized at the scene and sealed in a tamper evident package bearing a unique bar-coded seal number. This will be recorded along with details of the exhibits, and the sealed container signed and dated. IntaForensics will take custody of these seized items at the scene for imaging and processing back in the laboratory. IntaForensics will implement an 'exhibit custody authorisation form' which is currently provided to a number of existing clients, which will record details of all such exhibits seized. A copy will be provided to the NCFU Investigator and the owner of the equipment once this has been completed. Seized items will then be securely transported to IntaForensics' laboratory and handled in accordance with all normal policies and procedures. Transportation will be provided by one of the company's analysts, or dedicated IntaForensics security cleared logistics driver in a tracked and unmarked vehicle.

Upon arrival at the laboratory, the Duty Analyst will complete the collection record, scan and log the documentation onto Lima and assign the exhibits to a uniquely referenced location in the secure exhibits store. This store is proximity access controlled and is only accessible to operational staff. All evidential materials are stored in the secure exhibit storage with all interactions with the exhibit or forensic image recorded within IntaForensics' Lima Case Management system. This system allows IntaForensics to provide a full audit trail and ensure that there is a documented chain of custody.

Once back at the forensic laboratory, the processing team will commence imaging and preparing the exhibits for processing. This will include taking pictures of the exhibits and adding the initial details onto the Lima case; PIN codes will need to be supplied for the iPhone device. The MacBook devices will be imaged using MacQuisition, whilst the remaining devices will be imaged with FTK. As part of the case requirements, NFCU will provide IntaForensics with a keyword list for searching across the material. The processing team will enter the keywords into the system and process the exhibits. The result will be a full list of hits and matches for the keywords across the exhibits. It is at this stage that the exhibits and the keyword matches will be pre-analysed to the agreed limits by the analysts. NFCU will be updated by the analysts on the initial findings from the triage and processing of keywords. The NAS backups hold potentially key evidence due to the South American beef being labelled as British. In terms of providing the data to the labelling company this can be completed in a number of ways. The easiest would be to clone and then hash the NAS drives if they are used solely for that purpose. Alternatively, relevant files could be extracted and provided in a format of the client's choosing.

During the examination of the seized devices, if a standard method has failed to complete an examination or is known to be ineffective, an analyst can attempt a new examination or test method (outside the scope of ISO/IEC 17025), based on guidance from reputable sources of information and technical experience. This will be clearly documented in the Lima Forensic Case Management system, and endorsed by a Senior Analyst or Operations Management, and where the new examination or test proves successful, it should be repeated where possible to provide some degree of assurance. NFCU will be consulted for agreement regarding the use of any non-standard method before it is carried out.

IntaForensics offer varying turnaround times to their clients and this will be discussed and agreed during the work order requirement and forensic strategy meetings. For urgent times, this can be 7 days from the collection of data to the production to a technical report or witness statement. Less urgent cases can be conducted on 14 or 28-day turnaround times. Should the NFCU need to halt or cancel the examination or operation then this will need to be communicated to the SPoC and account manager as soon as possible. Timesheets will be reviewed and the NFCU will only be billed for the time spent on the case so far.

Upon completion of the processing, keyword searches and pre-analysis phases, IntaForensics will conduct a de-duplication exercise. This process is invaluable as when dealing with larger data sets it is extremely common for multiple documents containing the exact same matches to be flagged. An example of this would be a document saved in both a.doc and .pdf format. This would indicate 2 (two) matches, when in fact it is the same document. This exercise can dramatically reduce the amount of material that the investigators will need to review. IntaForensics will always take direction from NFCU on the scope of this exercise, with an agreed remit defined in the SLA or within a specific forensic strategy.

Once the de-duplication exercise has been concluded, the forensic team will communicate with the legal department representing the organisation to commence the Legal Professional Privilege Material review. The review platform will be implemented and configured for their role with support provided over the telephone. It is estimated that this review could take between 20-30 days during which time the legal team would review the data and highlight information they identify to fall under the category of LPP. Any items marked as LPP will not be visible or shared to the NFCU as part of the review package they receive.

When the company's legal team has conducted a full LPP review and bookmarked the areas they identify as LPP, IntaForensics will produce evidential packages in line with the Criminal Procedure and Investigations Act (CPIA) and Disclosure rules which are tailored specifically to the NFCU requirements. The package will contain a technical report by the expert, complete with an electronic copy of the evidence provided, unless produced on the online review platform. The format for reports and the presentation of media would be agreed with the NFCU as part of the Contract Mobilisation Plan and detailed in the bespoke SLA that is created for all clients; further considerations will be made during these meetings to agree on the format of court documents. IntaForensics can provide exhibit packages in hard copy, video and electronic formats as required; direction will be taken from the NFCU on the format they desire, please note that the size of data sets may restrict hard copy use. IntaForensics can, if required, provide disclosure packages to defence teams once this has been authorised by the NFCU. The protocols for this can be incorporated into the SLA which is defined during the Contract Mobilisation period. The company is experienced at dealing with defence teams on behalf of law enforcement agencies across the UK to provide authorised disclosures of required materials.

IntaForensics, using AccessData's AD Lab will create a review package for NFCU investigators. The review platform module called Quin-C will provide NFCU with the ability to conduct a full review and search across the data; the team will also create individual NFCU investigator access which will be tailored to their

role. This means that an NFCU investigator from Location 2 can see data and results from the exhibits seized and examined from Location 2, the same can be created for the other locations as well as access to all exhibits from all locations. Cross-case search is also available which will allow the investigators to search and report on links between suspects, including their contact history. NFCU investigators will also be able to create and export searchable PDF's from the native files in the system, giving the investigators the tools to quickly prepare reports in readable formats, if required for court or disclosure purposes.

IntaForensics will provide the NFCU at the end of this operation with either a Streamlined Forensic Report (SFR'S), MG11 Witness Statement and/or an Expert Technical Report. The company has conducted in excess of 17,000 cases, the vast majority of which have required either an MG11, SFR or Expert Technical Report. A significant number of these cases have resulted in a request for the analyst to prepare documentation and attend court anywhere in the UK to provide evidence and be cross-examined by both Prosecution and Defence. IntaForensics possesses staff that have a wealth of experience of presenting evidence at court, with a significant number of experts coming from key industrial backgrounds such as law enforcement and the military. The company is frequently contacted by witness care units around the UK to request and arrange court attendances for experts on a wide range of cases that have been examined.

IntaForensics can retain archives of case materials for periods to be agreed with the client, agreed during the mobilisation process. Typically, IntaForensics will hold the data for a period of between 30-60 days, at which point these will be returned to the client (at cost) or alternatively wiped using Tableau TD2 software upon NFCU instruction. Paper records are scanned and filed with the relevant archives, with paper records securely shredded and disposed of.

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

As a licensed Payment Card Forensic Investigation (PFI) company, IntaForensics has extensive experience in analysing remote assets such as AWS and Azure. The company utilises a variety of different specialist software products to forensically acquire cloud-based data. These include:

- Nuix
- UFED Cloud Analyzer
- F-Response

The tools that the analyst will select are driven by the IT infrastructure, data platform and the requirements of the client/officer. Where 'Enterprise' level target data (e.g. Exchange 365 hosted email server) is identified, the team use suitable administrator account credentials to obtain the whole server's data using a forensic collection tool, such as Nuix, at a central location. If a single administrator account is not available, the team would generate a PST for each target mailbox using PowerShell to interface with the hosted email sever and a forensic acquisition tool from hosts attached to the network (on-site).

For personal/individuals' Cloud-based data (e.g. DropBox, Gmail, iCloud), checks will be performed of any running hosts to establish if Cloud data is currently accessible and logical forensic images will be generated using X-Ways or EnCase. For Cloud accounts where credentials have been provided and

THE SCENARIO - PLAN AND DELIVERABLES

A. The Plan

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

IntaForensics has extensive experience of being involved in project planning from an early stage and has played a key part in providing strategic and project guidance for such search warrants for existing customers, such as the NCA and CMA. A detailed project plan is included below, however the company also provide examples of the value that can be added across the life of the framework, such as:

IntaForensics can assist in identifying likely sources of evidence dependant on locations in the premises, type of device, storage size etc.
IntaForensics can conduct a briefing or awareness training for NFCU investigators on the potential sources of data and handling of the exhibits in order to preserve live data
IntaForensics will advise on the appropriate data acquisition processes and the use of suitable forensic tools in the operation
IntaForensics will deploy analysts to support NFCU investigators depending on the location of exhibits of interest

Number	Task Details	Owner	Comments
1.0	Create case requirement	IntaForensics Submissions	Upon receipt of the work package from NFCU. The submission team will create the case requirement on the Lima case management system.

2.0	Assign work order to forensic team	IntaForensics Submissions	Submissions team will assign case to a Principal or Senior analyst in the laboratory for them to review and create a strategy.
2.1	Forensic strategy created	Principal / Senior Expert	Expert will review the work package and formulate a forensic strategy.
2.2	Forensic strategy submitted to NCFU	Principal / Senior Expert	Forensic strategy will be submitted to the NFCU for review and authorisation.
2.3	Authorise forensic strategy	NFCU	NFCU to authorise the forensic strategy.
2.4	Commercial arrangements and approval	NFCU & IntaForensics account manager	Based on initial estimates in the forensic strategy. NFCU approves the estimate of hours and commercial arrangements for IntaForensics to assist on the operation.
3.0	Arrange pre-deployment meeting	IntaForensics SPoC & NFCU	SPoC assigned and first task is to arrange a pre-deployment meeting with NFCU.
3.1	Identify locations	NFCU	NFCU to provide IntaForensics with the locations that are involved in the onsite operations. IntaForensics will use this information to be able to resource the requirement and place analysts on standby.
3.2	Identify digital media devices	NFCU	NFCU to provide IntaForensics with an overview of the expected types of media that might be found onsite.
3.3	Identify resources	IntaForensics SPoC	SPoC will coordinate with Forensic Operations Manager to identify resources to deploy onsite and support the operation.
3.4	Place resources on standby	SPoC & Operations	Identified resources will be placed on standby and logistical arrangements will be made, to include travel and accommodation.
4.0	Onsite Kit checks and prepare	SPoC / Sub-team Leaders	Lab staff to conduct a full review of onsite kits ready for deployment. SPoC will ensure that identified media types raised in the pre-deployment meeting are covered with forensic tools and that these are in the onsite kits.

5.0	Onsite deployment	NFCU & IntaForensics	Sub-teams deploy to the 3 locations alongside NFCU investigators to conduct warrants.
5.1	Onsite escalation and updates	SPoC & Ops Manager	SPoC and Ops Manager to provide first line support to the sub-teams and to ensure a clear line of communication and escalation route is managed with NFCU during the operation.
5.2	Onsite imaging and acquisition	Sub-teams	Sub-teams will conduct onsite acquisition and imaging of the servers found on scene.
5.3	Onsite seizure of devices	Sub-teams	Sub-teams will forensically seize the devices from the directors of the company
5.4	Return to Laboratory with devices	Sub-teams	Sub-teams will securely transport the forensic exhibits and image files back to the laboratory from the scene.
5.5	Enter exhibits into evidence store	Duty Analyst / Exhibit team	Once sub-teams arrive back at the lab, they will ensure that these are securely entered into the exhibit store and that the forensic case management is updated with the location of the exhibits.
6.0	Exhibit to be pre-imaged and processed	Processing Team	Processing team will retrieve the forensic exhibits from the store and pre-image these. The team will also commence the processing of the exhibits in line with the requirements.
6.1	Key word list to be supplied/reviewed/updated	NFCU	NFCU to supply IntaForensics with a keyword list to run across the acquired data sets.
6.2	Key word list entered into processing machine	Processing Team	Processing team will run keywords against the data acquired from the on-scene warrants.
7.0	Case assigned to forensic analyst for pre-analysis	Processing Team	Processing team to assign details over to a forensic analyst once the keywords have completed.
7.1	De-duplication exercise	Assigned Forensic Analyst	IntaForensics will conduct a de-duplication exercise on all positive matches to identify if any are the same documents and if there are multiple matches per document. This process will provide a

			streamlined output for LPP review and submission to NFCU.
7.2	LPP internal review and package created for company's' legal department	Legal Representative/Department	IntaForensics will provide an online review package to the company's legal representative/department for them to conduct a full and comprehensive LPP review, before returning their comments and bookmarked files to IntaForensics.
7.3	NFCU contacted with initial findings	Assigned Forensic Analyst	Forensic analyst to review findings and arrange an initial findings call with the NFCU. This can be done on a one-to-one basis with the investigator or as a group meeting call arranged by the SPoC.
7.4	Online review package completed	Assigned Forensic Analyst	Each Forensic analyst will create online review access for NFCU and share this with the SPoC and NFCU investigators.
7.5	NFCU conduct Investigation on review platform	NFCU Investigators	NFCU will conduct their investigation and review on the platform. NFCU may contact IntaForensics for support and questions during this project.
8.0	Report writing	Assigned Forensic Analyst	Each involved forensic analyst will generate a report for their involvement in the case,
8.1	Report QA (ISO/IEC 17025)	Assigned Forensic Analyst	Once the reports have been completed, the forensic analyst will assign a quality tasks for a peer review of the report before submitting the NFCU.
9.0	Completion of case requirements	Assigned Forensic Analyst	Final check of the case tasks before submitted case to the final stage of QA.
10.0	Dispatch of exhibits and reports	Forensic Analyst / Duty Analyst	Final QA conducted. Arrangements made with NFCU for the dispatch of exhibits and generated materials including the reports.

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 number or MILESTONE IN ORDER OF EXPECTED ACHIEVEMENT	**Target Date**	**TITLE of Deliverable or milestone**
1	Within 48 Hours (14/10/2020)	Submission of Forensic Strategy to NFCU **Deliverable for task 2.2**
2	19/10/2020	Pre-deployment Meeting **Deliverable for task 3.0**
3	20/10/2020	Coordinated deployment to onsite locations **Deliverable for task 5.0**
4	28/10/2020	De-duplication exercise **Deliverable for task 7.1**

5	30/10/2020	Generation of package for Legal team to conduct LPP review **Deliverable for task 7.2**
6	30/11/2020	Online review package completed **Deliverable for task 7.4**
7	31/12/2020	Technical report completed **Deliverable for task 8.0**
8	04/01/2021	MG11 Witness Statement completed **Deliverable for task 8.0**
9	04/01/2021	Dispatch of exhibits and reports to NFCU **Deliverable for task 10.0**
10	When required – could be up to 12 months after the case has concluded.	Court Preparation and attendance

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	IntaForensics Limited
Named staff members, details of specialism and expertise.	

IntaForensics has over 30 technical and analytical staff of various backgrounds and experience levels, located at the head office in Warwickshire. The team is comprised of Principal and Senior analysts, in addition to both mobile and computer dual-trained experts. For this scenario, IntaForensics would deploy the following staff across the locations specified. Please note that each work order will be reviewed and a forensic strategy will be provided, the staff resource will be tailored depending on the requirements and the expected type of devices/data medias.

Sean Daniel – Principal Forensic Analyst – SPoC, Project and Review Platform Manager

Sean has been a forensic expert for 8 years and has previously acted as the SPoC for CMA onsite engagements. Sean has extensive experience of conducting onsite operations and examining laptop and computer devices.

Christine Hall –Operations Manager – Escalation and Management Team

Christine has been a forensic expert for over 12 years, with an additional 4 years' experience as a forensic technician in law enforcement. Held supervisor and management roles for over 6 years and has a proven record of leading digital teams on large scale operations.

Adam Whitbread – Principal Forensic Analyst – HQ Onsite Computer Team

Adam has been a forensic expert since 2008, previously working for Leicestershire Police in their digital investigation unit. Adam has experience in seizing exhibits and conducting on-scene warrants.

Richard Inness – Principal Forensic Analyst – HQ Onsite Computer Team

Richard has been a forensic expert for over 10 years and has been involved extensively in onsite operations during this time. Richard has also held supervisor roles for the last 4 years and has experience in managing sub teams whilst conducting onsite duties.

Tamara Mason - Forensic Analyst – Location 1 Computer Team

Tamara has been a forensic analyst for over 3 years and has conducted onsite operations for the CMA previously. Tamara predominately conducts computer examinations and has been called to court on numerous occasions to provide evidence.

Ahzim Mir - Forensic Analyst – Location 1 Mobile Team

Ahzim has been a forensic analyst for 6 years and was significant in the onsite operations for the National Crime Agency (NCA). Ahzim is a dual trained analyst, equally skilled in conducting examinations on both computer and mobile devices.

Mary Geddes - Forensic Analyst – Location 2 Computer Team

Mary has been a forensic analyst for 4 years and was involved in the onsite operations for the CMA in 2019. Mary is predominately a computer forensic analyst, however, does provide assistance to IntaForensics Cell Site Survey team.

Adam Zia - Forensic Analyst – Location 2 Mobile Team

Adam has been a forensic analyst for 4 years and is the go-to expert for onsite mobile operations for the company's corporate/commercial clients. Adam predominately assists on investigations/examination involving mobile devices and has been called to court as an expert witness to provide evidence and face cross examination from both defence and prosecution.

Sam Duncombe – Senior Forensic Analyst – Computer Team

Sam has been a forensic analyst for over 5 years and has predominantly worked in law enforcement, assisting on onsite operations and imaging devices seized from suspects and victims. Sam has substantial experience in examining computer devices and is a senior forensic analyst with IntaForensics.

IntaForensics Processing Team – Pre-imaging and forensic processing all seized exhibits

The processing team at IntaForensics comprises 5 forensic analysts. Their main role is to pre-image all forensic exhibits and subsequently ensure the exhibits are processed before being assigned to a forensic analyst for examination and reporting.

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
Sean Daniel – SPoC. Project and Review Platform Manager	184 hours
Christine Hall – Management/Escalation	16 hours
Adam Whitbread - Principal Expert HQ	24 hours
Richard Inness - Principal Expert HQ	24 hours
Tamara Mason - Forensic Analyst Location 1	16 hours
Ahzim Mir - Forensic Analyst Location 1	16 hours
Mary Geddes - Forensic Analyst Location 2	16 hours
Adam Zia - Forensic Analyst Location 2	20 hours
Sam Duncombe – Forensic Analyst Computer	4 hours
Processing Team - IntaForensics Lab	16 hours
Total staff effort	336 Hours

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.

IntaForensics envisage that a notification will be received from NFCU of the requirement to deploy forensic support teams to three locations via a direct work order. IntaForensics will review the work requirements and assign a Principal or Senior forensic analyst to provide an initial forensic strategy. This initial forensic strategy will be provided to the NFCU within 48 hours of the work order submission. The dedicated Submissions team will be responsible for capturing the submission details, creating initial project tasks on the Lima management system, as well as ensuring that the forensic strategy is completed and submitted to NFCU within the agreed timeframes. The forensic strategy will detail the tools envisaged to be used on the operation and how they are incorporated in IntaForensics ISO/IEC 17025 scope of accreditation; should the company require tools that are outside the scope of ISO/IEC 17025, a detailed justification will be provided to NFCU. The forensic strategy will also include a commercial element, which will contain a breakdown of the hours estimated for the operation alongside a cost. The cost will be competitive and will strive to meet any budgetary requirements that the NFCU have.

Once the forensic strategy has been agreed by NFCU, IntaForensics will appoint a single point of contact (SPoC) for the project. The SPoC will be of Senior or Principal level and will be responsible for planning, communication and resolution activities throughout the whole project. This approach has been robustly tested previously during similar projects and successful outcomes demonstrate the effectiveness of having a SPoC for

engagements. The SPoC will work closely with the Forensic Operations Manager to identify the resources required for the project and to place these analysts “on standby”. The designated analysts will be assigned to the case on the Lima management system and the next stage of project tasks will be created and assigned to task owners within the case. A pre-deployment meeting will be organised by the SPoC, Forensic Operations Manager and NFCU prior to the onsite deployment. This meeting will involve a briefing by NFCU on issues such as PPE, hazards, approach to scene, timings and any other important areas of note that NFCU present. The meeting will allow the SPoC to understand the requirements and ensure that the coordination of the warrant is communicated to all involved. Finally, before the day of the warrant, the SPoC will ensure that all details are inputted on IntaForensics’ Lima management system. The SPoC will disseminate an offline package of the case to the analysts prior to the onsite attendance. Depending on NFCU’s preference, analysts can be issued with an offline package of the case management system to input exhibit details and notes. Alternatively, an exercise book can be provided to all analysts and then sealed in an evidence bag upon completion of the onsite engagement.

Analysts will deploy to their assigned locations to conduct the warrant alongside the NFCU investigators. The SPoC will maintain contact with each sub team throughout the day to resolve any challenges in addition to collating feedback to other sub and management teams. The SPoC will have contact information for NFCU contacts and will relay updates and initial onsite findings/results throughout the course of the on-scene attendances. Likewise, the SPoC can contact any of the sub-teams with all instructions/updates received from NFCU. It is anticipated that the attendances will need to be managed in a fluid manner as there is always the expectation that abnormalities may be encountered by the teams. The single point of contact with the NFCU will ensure that everyone can pivot and respond with alternative approaches whilst still achieving the desired results.

Each sub-team will be responsible for conducting their own acquisition processes onsite and will also be required to seize devices from the directors. These devices will be sealed into evidence bags and taken into the analyst’s custody. The sub team will ensure that these devices are transported securely to the head office forensic laboratory where they will be entered into the Lima system and the exhibit store. Once the exhibits have been processed and triaged in the forensic laboratory, the analysts will run keyword searches across the data sets. These keyword searches will be agreed as part of the forensic strategy initial and then defined once the on-scene attendances have been completed. The SPoC will be responsible for relaying any amendments or changes made to the key words by NFCU to the involved analysts.

Online review packs will be created by each analyst and communicated via the SPoC to the NFCU, any assistance and support will be provided by available analysts when requested. The SPoC and forensic technicians will prepare the exhibits and physical generated materials for dispatch to the NFCU or to the owner of the devices. Custody records will be updated on Lima and print outs can be provided to NFCU to show the full chain of custody of the exhibits in this project. Reports and witness statements will either be provided in physical copy via secure transport to NFCU or via secure email message. Any court attendances and requirements will be communicated to the IntaForensics Submissions team, who manage all court attendance requests and queries for the company.

A follow up meeting will be arranged with NFCU to discuss the project, understand any difficulties, feedback on the approaches that especially went well and to identify any further queries or follow up actions that may be required.

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 be taken to minimise these risks and how they will be managed by the project team. Please add more lines as required			
Identified risk	**Likelihood of risk (high, medium, low)**	**Impact of Risk (high, medium, low)**	**Risk management strategy**
Digital devices found on scene differ to the ones expected to be encountered	Medium	Medium	All forensic onsite operations are planned to handle different types of media, such as mobile phones and computers. Forensic onsite kits contain a selection of imaging tools and can cater for both computer and mobile devices. In the event of more devices being discovered then this can impact the time on scene due to the volume of the data being captured.
Evidence accessed during transit could result in a loss of confidentiality and case related data. This impacts the chain of custody and will compromise the integrity of the data and exhibits.	Low	High	The IntaForensics Operations Management team ensure that this risk is managed by ensuring that strict exhibit continuity and chain of custody processes are in place, as well as having secure delivery vehicles (GPS tracked) and trained staff. Exhibits will be placed into sealed tamper evident transit bags and containers as well as a full track and trace process for all exhibits outside of IntaForensics premises. Drives will be encrypted for transit to ensure no unauthorised access is allowed.
Problems with software and forensic tools not functioning correctly or as expected as per the vendors specification which can mean Information relevant to the case is not available for processing and analysis.	Low	Medium	A robust validation programme is implemented at IntaForensics which involves testing and challenging the applications in operation within the laboratory. Isolated validation workstations constructed to reflect the operation are facilitated to identify any conflicting applications. Onsite kits are regularly checked and validated to ensure that the tools are problem free and up to date.
During an onsite activity, a number of risks are identified. These are:	Low	High	Operations Management tackle this risk by ensuring that onsite operations follow a structured deployment process which is

• Potential loss of security • Exposure of assets • Potential unauthorised access to data/information/equipment • Potential physical risks to staff			carried out in accordance with instructions from the OIC (client). Dedicated equipment and onsite kits are prepared and ready for deployment when required. Documented processes and procedures are in place for onsite activity, IF-SOP-39.

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**
Example – Data Associated with MS Windows	*Example -Forensic Analysis and extraction from digital media*	*Example - Documented methods using 3rd party software and hardware - FTK*	*Example - In house SOP 1, 2, 3, 4*
Computers and digital storage devices: • Hard disk drives • Solid state drives • Memory cards • USB flash drives • Compact discs • Digital versatile discs • Digital cameras • Floppy disks	Physical capture and preservation of data	Documented in-house methods using: • Guidance EnCase • AccessData FTK Imager • CAINE Guymager • Guidance Tableau T356789lu • Guidance Tableau T35u • Guidance Tableau T35is • Guidance Tableau TD2	In-house SOP's: • LAB-SOP-04 • LAB-SOP-05 • LAB-SOP-12 CD/DVD • LAB-SOP-21 Memory Cards • LAB-SOP-33 Floppy Disks • LAB-SOP-40 CAINE • LAB-SOP-45 USB devices
Computers and digital storage devices:	Physical capture and preservation of data	Documented in-house methods using:	In-house SOP

• Hard disk drives • Solid state drives		BlackBag MacQuisition	• LAB-SOP-39 MacQuisition
Digital devices and data, computers Data associated with the following: • Microsoft Windows • macOS	Processing and analysis of data	Documented in-house methods using: • Guidance EnCase • Magnet IEF • Griffeye Analyze with Blue Bear LACE Carver	In-house SOP's: • LAB-SOP-22 • LAB-SOP-62
Drones Drones (Unmanned Aerial Vehicle) • DJI • PARROT	Physical capture and preservation of data	Documented in-house methods using: • MSAB XRY • Cellebrite UFED 4PC • AccessData FTK Imager	In-house SOP: • LAB-SOP-63
	Logical capture and preservation of data	Documented in-house methods using: • MSAB XRY • Cellebrite UFED 4PC	
	Processing of data	Documented in-house methods using: • MSAB XRY • MSAB XAMN • Cellebrite UFED Physical Analyzer	

Mobile Phones Mobile phone handsets and tablets associated with the following operating systems: • Google Android • Non-Smartphone proprietary systems	Physical capture and preservation of data	Documented in-house methods using: • MSAB XRY • Cellebrite UFED 4PC	In-house SOP's: • LAB-SOP-24 • LAB-SOP-25
Mobile phone handsets and tablets associated with the following operating systems: • Apple iOS • Google Android • Non-smartphone proprietary systems	Logical capture Processing of data	Documented in-house methods using: • MSAB XRY • Cellebrite UFED 4PC • Manual examination Documented in-house methods using: • MSAB XRY • MSAB XAMN • Cellebrite UFED Physical Analyzer • SQLite Expert Professional	In-house SOP's • LAB-SOP-24 • LAB-SOP-25

(U) Sim cards	Logical capture and preservation of data Processing of data	Documented in-house methods using: • MSAB XRY • Cellebrite UFED 4PC • Cellebrite UFED Touch2 Documented in-house methods using: • MSAB XRY • MSAB XAMN • Cellebrite UFED Physical Analyzer	In-house SOP • LAB-SOP-49 SIM Cards
Satellite navigation systems Satellite navigation systems associated with the following manufactures / systems: • Garmin • TomTom	Physical capture and preservation of data Logical capture preservation of data	Documented in-house methods using: • AccessData FTK Imager Documented in-house methods using: • Manual examination	In-house SOP • LAB-SOP-53

INVESTIGATIVE REVIEW PLATFORM

In the below space please give accurate details of what Investigative review platform will be provided with the package 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

Upon award of a place on the framework, IntaForensics will undertake to fully implement AccessData's AD Lab solution. AD Lab is built on FTK® technology and is an investigative platform, featuring numerous modules that enable IntaForensics to define individual roles across large scale investigations. A centralised database controlled, administrated, and operated 'on premise' by IntaForensics will allow multiple investigators to conduct web and desktop review activities on significant data sizes. IntaForensics have held advanced conversations with AccessData and once a place on the framework has been confirmed, IntaForensics will implement the system – we envisage this deployment to not take longer than a couple of weeks. It is important to note, that IntaForensics also use NUIX currently in the forensic laboratory however the company feels that the NUIX platform does not provide the robustness and user-friendly system that AD Lab does. IntaForensics prides itself on high levels of customer satisfaction and feel that the AD Lab solution will significantly improve the end investigator experience of using the platform for extremely important investigations. However, should the NFCU request the NUIX platform, then IntaForensics can offer this as a service. The AD Lab solution has been designed to be user-friendly for non-technical users should they also be required to access the system. Users of the solution can effortlessly configure and adapt the weighting criteria for searches across the data to reveal the most relevant results. Email notifications during case milestones can be created and tracked in an audit log feature in addition to chain of custody records.

Access to the system will be created and managed by IntaForensics. Multiple roles can be created for NCFU investigators,

meaning they have access to data that is only relevant to their part of the investigation. Roles and privileges will be discussed and agreed during the pre-deployment meeting, with notes inputted into the Lima case management system. NFCU investigators have the option of installing a desktop application or using web-based access, the platform supports both options and can provide NFCU with more flexibility with home workers. Multiple investigators will be able to access the system from numerous locations, and should an investigator need to review the details offline, they can simply export the case into a portable case for offline review. This removes the requirement for generating reports as the portable case provides a quick export.

IntaForensics intend to place a number of Principal and Senior analysts on AccessData's bespoke support and training program for the platform, this will mean that IntaForensics will be able to support the NCFU with the application during setup and investigation and, should any subsequent court requirements be required. Support will be offered to the NFCU in first line telephone support up to in person meetings should this required. IntaForensics envisage that due to the simplified user interface of the system, issues requiring support will mainly be resolved over the phone, however on site in person support can be provided if required.

The platform is hosted onsite at IntaForensics on a secure network behind multiple firewalls. The company has a 1GB line connected directly to the internet, therefore it is unlikely that there will be any network disturbance or latency. This method significantly reduces the cost of an e-discovery platform as data is not being downloaded from the cloud such as AWS.

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 into 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)

Appendix A – ISO 9001

Appendix B – ISO/IEC 27001

Appendix C – ISO/IEC 17025

Appendix D – ISO 14001

Appendix E – CE & CE+

Appendix F – IF-SOP-35 – Legal Professional Privilege Policy v1_0

Appendix G – LAB-SOP-09 – Hard Disk Wiping Procedure v1_3

Appendix H – LAB-SOP-18 – Case Archive Procedure v1_6

Appendix I – Self-Cleansing Response to Question 3.1 (d) of SQ – **NOT IN ZIP FOLDER – Submitted as part of SQ**

Appendix J – Gantt Chart for The Scenario Question A – The Plan

Clarifications Questions and Answers

Q1. There is a willingness to help the NFCU with awareness training being offered, but does this come at a cost?

A1. IntaForensics will offer ‘Forensic Awareness & Review Platform Training’ and whilst the costs to deliver this will be free of charge to the FSA and as part of project delivery, it must be offset against framework revenue. Therefore, providing the FSA are actively using IntaForensics to deliver investigative and forensic services, the company will deliver this service on a bi-annual basis, or more frequently dependant on service usage, free of charge.

Q2. If Nuix is used, as an alternative to Quin C will there be any additional charges for licences?

A2. We have selected the AccessData platform as being the most versatile and economical for the requirements of the FSA and have fully costed this in our response. IntaForensics will train and support online and offline investigations by FSA investigators to ensure that any transition is as transparent as possible and, in addition, will offer 24/7 support to FSA (NFCU) during any investigation. We can confirm that based on the 'sample project' and the assumptions we have made on the LPP Review and FSA online reviewer volume, no further costs are required to provide NUIX as an alternative.

Q3. Some further justification and explanation is required in relation to the number of hours allocated to the SPOC, do these hours cover the full process rather than being separated out to other roles?

A3. With reference to the costs for the SPoC; whilst inferred as ‘management’, this role is also head of the technical delivery team on a project and our previous experiences have proved that this level of team integration enables the SPoC to be centric to all aspects of the project. The SpoC function is undertaken by a Principal Digital Forensic Analyst, not account management staff, and covers the full cost of the ‘sample project’ investigation. As answered in the scenario question (plan and deliverables) and shown in the project plan, the SPOC has full oversight of the project and will provide support during the larger elements of the scenario (LPP review by legal team and NFCU investigation on review platform). Based on the requirements in the scenario we have provided estimates of time and, as always, only time recorded against the project in our case management system will be billed and made available as transparency data to the FSA at the point of billing. IntaForensics have a proven track record of providing an economical and sustainable service with full transparency.

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.
- 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 off the RFQ. 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 each Category of Personal Data	**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 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	*[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 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	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*
Categories of Data Subject	*[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	*[Describe how long the data will be retained for, how it be returned or destroyed]*

Completed by:
Date:
Call Off - Work package award acceptance
Date quotation accepted by FSA:
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;

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.

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.

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 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)
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, 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 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.

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.

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

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).

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;

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.

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.

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

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'.

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;

(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

(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.

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.

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;

(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;

(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.

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.

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).*

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.

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: **Andrew Frowen Andrew.Frowen@intaforeniscs.com**
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:

	• ***[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*

	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]*

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:

(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;

(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

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.

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]

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**"):

(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.

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]

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 .....

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.

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,

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.

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.

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;

(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.